LINKSYS®

A Division of Cisco Systems, Inc.

2.4GHz 802.11g

Wireless-G Portable USB Adapter User Guide

WIRELESS

Model No. **WUSB54GP**

CISCO SYSTEMS

Copyright and Trademarks

Specifications are subject to change without notice. Linksys is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. Copyright © 2004 Cisco Systems, Inc. All rights reserved. Other brands and product names are trademarks or registered trademarks of their respective holders.

WARNING: This product contains chemicals, including lead, known to the State of California to cause cancer, and birth defects or other reproductive harm. ***Wash hands after handling.***

This User Guide

The User Guide to the Wireless-G Portable USB Adapter has been designed to make understanding networking easier than ever. Look for the following items when reading this guide:

This checkmark means there is a note of interest and is something you should pay special attention to while using the Adapter.

This exclamation point means there is a caution or warning and is something that could damage your property or the Adapter.

This question mark provides you with a reminder about something you might need to do while using the Adapter.

word: *definition.*

In addition to these symbols, there are definitions for technical terms that are presented like this:

Figure 0-1: Sample Figure Description

Also, each figure (diagram, screenshot, or other image) is provided with a figure number and description, like this:

Figure numbers and descriptions can also be found in the “List of Figures” section in the “Table of Contents”.

Table of Contents

Chapter 1: Introduction 1
Welcome 1
What's in this Guide? 2
Chapter 2: Planning Your Wireless Network 4
Network Topology 4
Roaming 4
Network Layout 5
Chapter 3: Getting to Know the Wireless-G Portable USB Adapter 6
The USB Port 6
The LED Indicator 6
Chapter 4: Setting up the Wireless-G Portable USB Adapter 7
Using the Setup Wizard 7
Chapter 5: Connecting the Wireless-G Portable USB Adapter 14
Using the USB Extension Base 15
Using the Adapter's Wall Mount 16
Chapter 6: Using the Wireless Network Monitor 17
Using the Wireless Network Monitor Icon 17
Accessing the Wireless Network Monitor 18
Link Information 18
Site Survey 21
Profiles 22
Creating a New Profile 23
Appendix A: Troubleshooting 30
Common Problems and Solutions 30
Frequently Asked Questions 31
Appendix B: Wireless Security 34
Security Precautions 34
Security Threats Facing Wireless Networks 34
Appendix C: Windows Help 37
Appendix D: Glossary 38
Appendix E: Specifications 45

Appendix F: Warranty Information 47
Appendix G: Regulatory Information 48
Appendix H: Contact Information 50

List of Figures

Figure 3-1: USB Port and Cord 6
Figure 3-2: Front Panel 6
Figure 4-1: Setup Wizard's Welcome Screen 7
Figure 4-2: Setup Wizard's License Agreement 7
Figure 4-3: Setup Wizard's Wireless Mode Screen 8
Figure 4-4: Setup Wizard's Ad-Hoc Mode Settings Screen 8
Figure 4-5: Setup Wizard's Wireless Security Screen 9
Figure 4-6: Setup Wizard's Wireless Security - WEP Screen 9
Figure 4-7: Setup Wizard's Wireless Security - PSK Using TKIP Screen 10
Figure 4-8: Setup Wizard's Wireless Security - PSK Using AES Screen 10
Figure 4-9: Setup Wizard's Wireless Security - PSK + RADIUS Using EAP-TLS Screen 11
Figure 4-10: Setup Wizard's Wireless Security - PSK + RADIUS Using PEAP Screen 11
Figure 4-11: Setup Wizard's Wireless Security - RADIUS Using EAP-TLS Screen 12
Figure 4-12: Setup Wizard's Wireless Security - RADIUS Using PEAP Screen 12
Figure 4-13: Setup Wizard's Check Settings Screen 13
Figure 4-14: Digital Signature Not Found Screen 13
Figure 4-15: Setup Wizard's Congratulations Screen 13
Figure 5-1: The Portable USB Adapter on Your Notebook 14
Figure 5-2: A USB Port 14
Figure 5-3: Digital Signature Not Found Screen 15
Figure 5-4: Using the USB Extension Base 15
Figure 5-5: Using the Wall Mount 16
Figure 6-1: Wireless Network Monitor Icon 17
Figure 6-2: Windows XP - Use Windows XP Wireless Configuration 17
Figure 6-3: Windows XP - Use Linksys Wireless Network Monitor 17
Figure 6-4: Link Information 18
Figure 6-5: More Information - Wireless Network Status 19
Figure 6-6: More Information-Network Statistics 20
Figure 6-7: Site Survey 21
Figure 6-8: WEP Key Needed for Connection 21

Figure 6-9: PSK (Pre-Shared Key) Needed for Connection 21
Figure 6-10: Profiles 22
Figure 6-11: Import a Profile 22
Figure 6-12: Export a Profile 22
Figure 6-13: Create a New Profile 23
Figure 6-14: Enter Profile Name 23
Figure 6-15: Network Settings for New Profile 23
Figure 6-16: Wireless Mode for New Profile 24
Figure 6-17: Ad-Hoc Mode Settings for New Profile 24
Figure 6-18: Wireless Security for New Profile 25
Figure 6-19: Wireless Security - WEP for New Profile 25
Figure 6-20: Wireless Security - PSK for New Profile 26
Figure 6-21: Wireless Security - PSK + RADIUS Using EAP-TLS for New Profile 27
Figure 6-22: Wireless Security - PSK + RADIUS Using PEAP for New Profile 27
Figure 6-23: Wireless Security - RADIUS Using EAP-TLS for New Profile 28
Figure 6-24: Wireless Security - RADIUS Using PEAP for New Profile 28
Figure 6-25: Confirm New Settings for New Profile 29
Figure 6-26: Congratulations for New Profile 29

Chapter 1: Introduction

Welcome

Thank you for choosing the Wireless-G Portable USB Adapter. With this Adapter, your wireless networking experience will be faster and easier than ever.

How does the Adapter do this? Like all wireless products, the Adapter allows for greater range and mobility within your wireless network. Connecting to your PC via the USB port means that this Adapter leaves the PC's slots open for other purposes. This adapter communicates over the 802.11g wireless standard, one of the newest wireless standards, to communicate with your network.

But what does all of this mean?

Networks are useful tools for sharing computer resources. You can access one printer from different computers and access data located on another computer's hard drive. Networks are even used for playing multiplayer video games. So, networks are not only useful in homes and offices, they can also be fun.

PCs equipped with wireless cards and adapters can communicate without cumbersome cables. By sharing the same wireless settings, within their transmission radius, they form a wireless network.

Use the instructions in this Guide to help you connect the Adapter, set it up, and configure it for your network. These instructions should be all you need to get the most out of the Adapter.

network: *a series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users.*

adapter: *a device that adds network functionality to your PC.*

802.11g: *an IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps, an operating frequency of 2.4GHz, and backward compatibility with 802.11b devices.*

What's in this Guide?

This user guide covers the steps for setting up and using the Wireless-G Portable USB Adapter.

- Chapter 1: Introduction
  This chapter describes the Adapter's applications and this User Guide.
- Chapter 2: Planning Your Wireless Network
  This chapter discusses a few of the basics about wireless networking.
- Chapter 3: Getting to Know the Wireless-G Portable USB Adapter
  This chapter describes the physical features of the Adapter.
- Chapter 4: Setting up the Wireless-G Portable USB Adapter
  This chapter instructs you on how to run the Adapter's Setup Wizard and configure the Adapter.
- Chapter 5: Connecting the Wireless-G Portable USB Adapter
  This chapter shows you how to connect the Adapter to your PC.
- Chapter 6: Using the Wireless Network Monitor
  This chapter explains how to use the Adapter's Wireless Network Monitor.
- Appendix A: Troubleshooting
  This appendix describes some potential problems and solutions, as well as frequently asked questions, regarding installation and use of the Adapter.
- Appendix B: Wireless Security
  This appendix discusses security issues regarding wireless networking and measures you can take to help protect your wireless network.
- Appendix C: Windows Help
  This appendix describes how you can use Windows Help for instructions about networking, such as installing the TCP/IP protocol.
- Appendix D: Glossary
  This appendix gives a brief glossary of terms frequently used in networking.
- Appendix E: Specifications
  This appendix provides the Adapter's technical specifications.
- Appendix F: Warranty Information
  This appendix supplies the Adapter's warranty information.

- Appendix G: Regulatory Information
  This appendix supplies the Adapter's regulatory information.

- Appendix H: Contact Information
  This appendix provides contact information for a variety of Linksys resources, including Technical Support.

Chapter 2: Planning Your Wireless Network

Network Topology

A wireless network is a group of computers, each equipped with one wireless adapter. Computers in a wireless network must be configured to share the same radio channel. Several PCs equipped with wireless cards or adapters can communicate with one another to form an ad-hoc network.

Linksys wireless adapters also provide users access to a wired network when using an access point or wireless router. An integrated wireless and wired network is called an infrastructure network. Each wireless PC in an infrastructure network can talk to any computer in a wired network infrastructure via the access point or wireless router.

An infrastructure configuration extends the accessibility of a wireless PC to a wired network, and can double the effective wireless transmission range for two wireless adapter PCs. Since an access point is able to forward data within a network, the effective transmission range in an infrastructure network can be doubled.

Roaming

Infrastructure mode also supports roaming capabilities for mobile users. Roaming means that you can move your wireless PC within your network and the access points will pick up the wireless PC's signal, provided that they both share the same channel and SSID.

Choose a feasible radio channel and optimum access point position. Proper access point positioning combined with a clear radio signal will greatly enhance performance.

***ad-hoc**: a group of wireless devices communicating directly with each other (peer-to-peer) without the use of an access point*

***access point**: device that allows wireless-equipped computers and other devices to communicate with a wired network.*

***infrastructure**: Configuration in which a wireless network is bridged to a wired network via an access point.*

***roaming**: the ability to take a wireless device from one access point's range to another without losing the connection.*

***ssid**: your wireless network's name*

Network Layout

Linksys wireless access points and wireless routers have been designed for use with 802.11a, 802.11b, and 802.11g products. With 802.11g products communicating with the 802.11b standard and some products incorporating both “a” and “g”, products using these standards can communicate with each other.

Access points and wireless routers are compatible with 802.11a, 802.11b and 802.11g adapters, such as the PC Adapters for your laptop computers, PCI Adapters for your desktop PCs, and USB Adapters for when you want to enjoy USB connectivity. Wireless products will also communicate with the Wireless PrintServer.

When you wish to connect your wired network with your wireless network, network ports on access points and wireless routers can be connected to any of Linksys's switches or routers.

With these, and many other, Linksys products, your networking options are limitless. Go to the Linksys website at *www.linksys.com* for more information about wireless products.

802.11g: *an IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps, an operating frequency of 2.4GHz, and backward compatibility with 802.11b devices.*

switch*: device that is the central point of connection for computers and other devices in a network, so data can be shared at full transmission speeds.*

router*: a networking device that connects multiple networks together, such as a local network and the Internet.*

Chapter 3: Getting to Know the Wireless-G Portable USB Adapter

The USB Extension Base

The USB port is located on the USB Estension Base. If desired, you can attach the Adapter here and attach the connector to the PC.

Figure 3-1: USB Extension Base and Cord

The LED Indicator

The Adapter's LED indicates the status of the Adapter's wireless connection.

Figure 3-2: Front Panel

Link *Blue* The Link LED lights up when the Adapter has an active wireless connection. It will flash when data is transmitted.

Chapter 4: Setting up the Wireless-G Portable USB Adapter

The Wireless-G Portable USB Adapter Setup Wizard will guide you through the installation procedure. The Setup Wizard will install the driver and Wireless Network Monitor, as well as configure the Adapter.

NOTE: You must run the Setup Wizard before connecting the Adapter to your computer.

Using the Setup Wizard

Insert the **Setup Wizard CD-ROM** into your CD-ROM drive. The Setup Wizard should run automatically, and the *Welcome* screen should appear. If it does not, click the **Start** button and choose **Run**. In the field that appears, enter **D:\setup.exe** (if "D" is the letter of your CD-ROM drive).

LINKSYS
A Division of Cisco Systems, Inc.
Welcome
Welcome to the Setup Wizard for the Wireless-G Portable USB Adapter.
To function properly, the Adapter's software should be installed from this disk before connecting the Adapter. Click the Install button to begin.
2.4GHz 802.11g Wireless-G
Portable USB Adapter Setup Wizard ver. 4.0
Install | User Guide | Exit
Cisco Systems
Model No. WUSB54GP Copyright © 2004 Cisco Systems, Inc. All rights reserved.

Figure 4-1: Setup Wizard's Welcome Screen

On the *Welcome* screen, you have the following choices:

Install - Click the **Install** button to begin the software installation process.

User Guide - Click the **User Guide** button to open the PDF file of this User Guide.

Exit - Click the **Exit** button to exit the Setup Wizard.

1. To install the Adapter, click the **Install** button on the *Welcome* screen.
2. After reading the License Agreement, click the **Next** button if you agree, or click the **Cancel** button to end the installation.

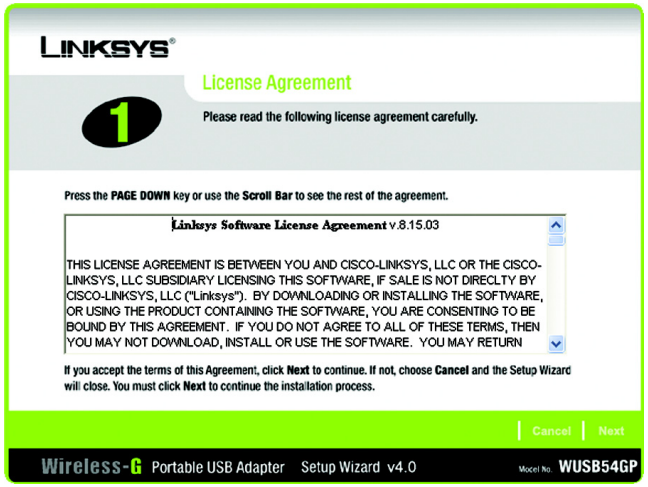
LINKSYS
License Agreement
1
Please read the following license agreement carefully.
Press the PAGE DOWN key or use the Scroll Bar to see the rest of the agreement.
Linksys Software License Agreement v.8.15.03
THIS LICENSE AGREEMENT IS BETWEEN YOU AND CISCO-LINKSYS, LLC OR THE CISCO-LINKSYS, LLC SUBSIDIARY LICENSING THIS SOFTWARE, IF SALE IS NOT DIRECLTY BY CISCO-LINKSYS, LLC ("Linksys"). BY DOWNLOADING OR INSTALLING THE SOFTWARE, OR USING THE PRODUCT CONTAINING THE SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THESE TERMS, THEN YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE. YOU MAY RETURN
If you accept the terms of this Agreement, click Next to continue. If not, choose Cancel and the Setup Wizard will close. You must click Next to continue the installation process.
Cancel | Next
Wireless-G Portable USB Adapter Setup Wizard v4.0
Model No. WUSB54GP

Figure 4-2: Setup Wizard's License Agreement

3. The Setup Wizard will ask you to choose a network mode. Click the **Infrastructure Mode** radio button if you want your wireless computers to network with computers on your wired network using a wireless access point. Click the **Ad-Hoc Mode** radio button if you want multiple wireless computers to network directly with each other.

   In the *SSID* field, enter the SSID of your wireless network. The SSID must be identical for all devices in the network. The default setting is **linksys** (all lowercase) for the Adapter, Linksys access points, and wireless routers. Click the **Next** button.

NOTE: Network SSIDs should be unique to your network and identical for all devices within the network.

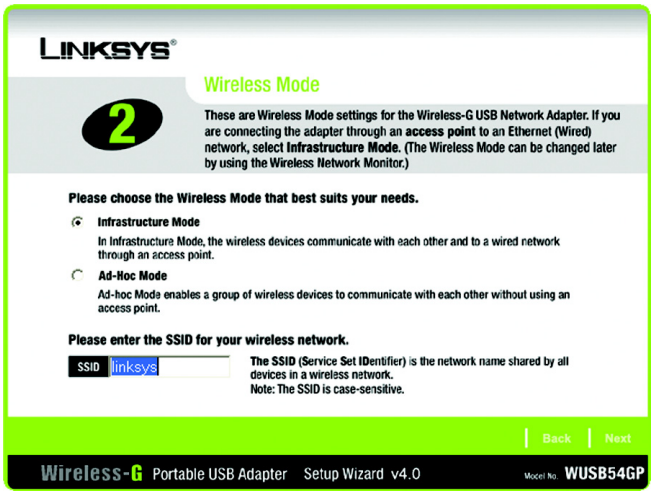
LINKSYS
Wireless Mode
2
These are Wireless Mode settings for the Wireless-G USB Network Adapter. If you are connecting the adapter through an access point to an Ethernet (Wired) network, select Infrastructure Mode. (The Wireless Mode can be changed later by using the Wireless Network Monitor.)
Please choose the Wireless Mode that best suits your needs.
Infrastructure Mode
In Infrastructure Mode, the wireless devices communicate with each other and to a wired network through an access point.
Ad-Hoc Mode
Ad-hoc Mode enables a group of wireless devices to communicate with each other without using an access point.
Please enter the SSID for your wireless network.
SSID linksys
The SSID (Service Set IDentifier) is the network name shared by all devices in a wireless network.
Note: The SSID is case-sensitive.
Back
Next
Wireless-G Portable USB Adapter Setup Wizard v4.0
Model No. WUSB54GP

Figure 4-3: Setup Wizard's Wireless Mode Screen

4. If you chose **Infrastructure Mode**, go to Step 5 now. If you chose **Ad-Hoc Mode**, select the correct operating channel for your network. Then, select the Network Mode from the drop-down menu. Click the **Next** button, and go to Step 5. Click the **Back** button to change any settings.

   Channel - The channel you choose should match the channel set on the other devices in your wireless network. If you are unsure about which channel to use, select the default channel (Channel 6).

   Network Mode - Select **Mixed Mode** if you want to allow Wireless-G and Wireless-B computers on the network, even though network speeds will be reduced. For maximum speed, select **G-Only Mode**; however, no Wireless-B users will be allowed on the network.

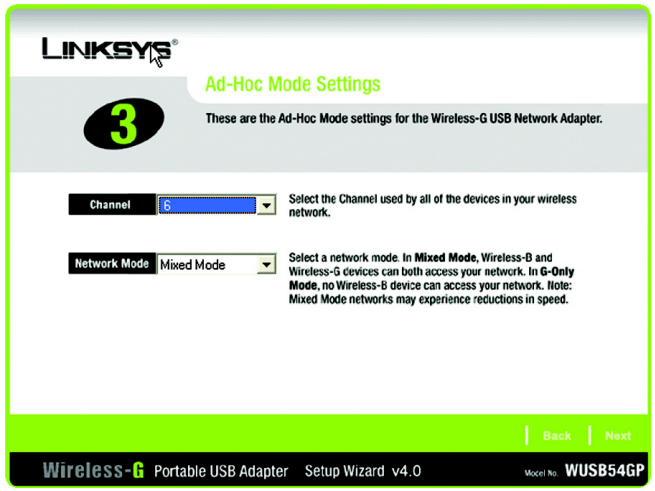
LINKSYS
Ad-Hoc Mode Settings
3
These are the Ad-Hoc Mode settings for the Wireless-G USB Network Adapter.
Channel 6
Select the Channel used by all of the devices in your wireless network.
Network Mode Mixed Mode
Select a network mode. In Mixed Mode, Wireless-B and Wireless-G devices can both access your network. In G-Only Mode, no Wireless-B device can access your network. Note: Mixed Mode networks may experience reductions in speed.
Back
Next
Wireless-G Portable USB Adapter Setup Wizard v4.0
Model No. WUSB54GP

Figure 4-4: Setup Wizard's Ad-Hoc Mode Settings Screen

5. Select the method of security you want to use: **WEP**, **PSK**, **PSK + RADIUS**, or **RADIUS**. WEP stands for Wired Equivalent Privacy, and PSK stands for Pre-Shared Key. RADIUS stands for Remote Authentication Dial-In User Service.

NOTE: If your network is using WPA-Personal or WPA-PSK security, then select **PSK**. If your network is using WPA-Enterprise or WPA-RADIUS security, then select **PSK + RADIUS**.

If you don't want to use encryption, select **Disabled** and then click the **Next** button to continue. Proceed to Step 7.

Click the **Next** button to continue or the **Back** button to return to the previous screen.

6. Proceed to the appropriate section for your security method: WEP, PSK, PSK-RADIUS, or RADIUS.

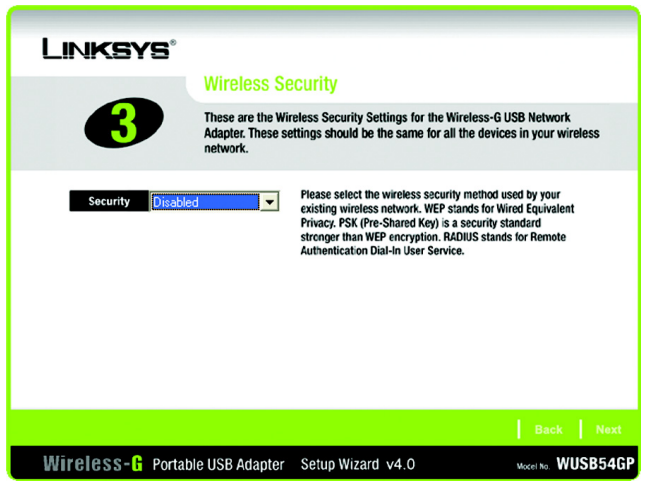
LINKSYS
Wireless Security
3
These are the Wireless Security Settings for the Wireless-G USB Network Adapter. These settings should be the same for all the devices in your wireless network.
Security
Disabled
Please select the wireless security method used by your existing wireless network. WEP stands for Wired Equivalent Privacy. PSK (Pre-Shared Key) is a security standard stronger than WEP encryption. RADIUS stands for Remote Authentication Dial-In User Service.
Back
Next
Wireless-G Portable USB Adapter Setup Wizard v4.0
Model No. WUSB54GP

Figure 4-5: Setup Wizard's Wireless Security Screen

WEP

WEP - Select **64-bit** or **128-bit** encryption from the drop-down menu, and enter a passphrase or WEP key.

Passphrase - Enter a passphrase in the *Passphrase* field, so a WEP key is automatically generated. It is case-sensitive and should not be longer than 16 alphanumeric characters. This passphrase must match the passphrase of your other wireless network devices and is compatible with Linksys wireless products only. (If you have any non-Linksys wireless products, enter the WEP key manually on those products.)

WEP Key - The WEP key you enter must match the WEP key of your wireless network. For 64-bit encryption, enter exactly 10 hexadecimal characters. For 128-bit encryption, enter exactly 26 hexadecimal characters. Valid hexadecimal characters are "0" to "9" and "A" to "F".

Advanced Users

TX Key - The default transmit key number is 1. If your network's access point or wireless router uses transmit key number 2, 3, or 4, select the appropriate number from the *TX Key* drop-down box.

Authentication -The default is set to **Auto**, so it will auto-detect for **Shared Key** or **Open System** authentication. For Shared Key authentication, both the sender and the recipient share a WEP key for authentication. For Open System authentication, the sender and the recipient do not share a WEP key for authentication. If you are not sure which authentication method to select, keep the default, **Auto**.

Click the **Next** button to continue. Click the **Back** button to return to the previous screen.

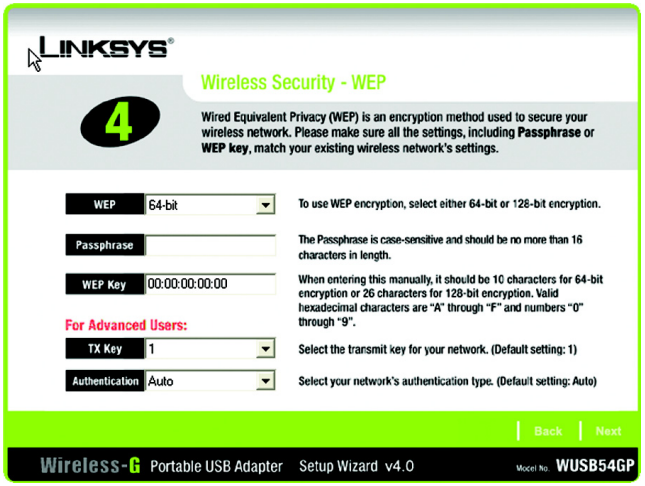
LINKSYS
Wireless Security - WEP
4
Wired Equivalent Privacy (WEP) is an encryption method used to secure your wireless network. Please make sure all the settings, including Passphrase or WEP key, match your existing wireless network's settings.
WEP
64-bit
To use WEP encryption, select either 64-bit or 128-bit encryption.
Passphrase
The Passphrase is case-sensitive and should be no more than 16 characters in length.
WEP Key
00:00:00:00:00
When entering this manually, it should be 10 characters for 64-bit encryption or 26 characters for 128-bit encryption. Valid hexadecimal characters are "A" through "F" and numbers "0" through "9".
For Advanced Users:
TX Key
1
Select the transmit key for your network. (Default setting: 1)
Authentication
Auto
Select your network's authentication type. (Default setting: Auto)
Back
Next
Wireless-G Portable USB Adapter Setup Wizard v4.0
Model No. WUSB54GP

Figure 4-6: Setup Wizard's Wireless Security - WEP Screen

PSK

PSK offers two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **TKIP** or **AES**, for the *Encryption Type*. Then enter a Passphrase that is 8-63 characters in length.

Encryption - Select the type of algorithm you want to use, **TKIP** or **AES**, for the *Encryption Type*.

Passphrase - Enter a Passphrase, also called a Pre-Shared Key, of 8-63 characters in the *Passphrase* field. The longer and more complex your Passphrase is, the more secure your network will be.

Click the **Next** button to continue. Click the **Back** button to return to the previous screen.

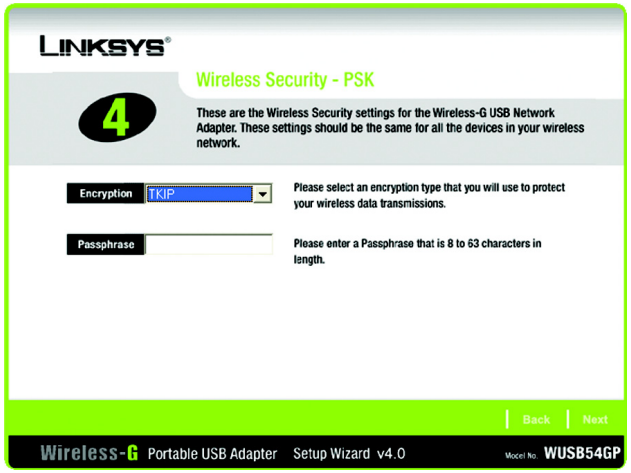
LINKSYS
Wireless Security - PSK
4
These are the Wireless Security settings for the Wireless-G USB Network Adapter. These settings should be the same for all the devices in your wireless network.
Encryption
TKIP
Please select an encryption type that you will use to protect your wireless data transmissions.
Passphrase
Please enter a Passphrase that is 8 to 63 characters in length.
Back
Next
Wireless-G Portable USB Adapter Setup Wizard v4.0
Model No. WUSB54GP

Figure 4-7: Setup Wizard's Wireless Security - PSK Using TKIP Screen

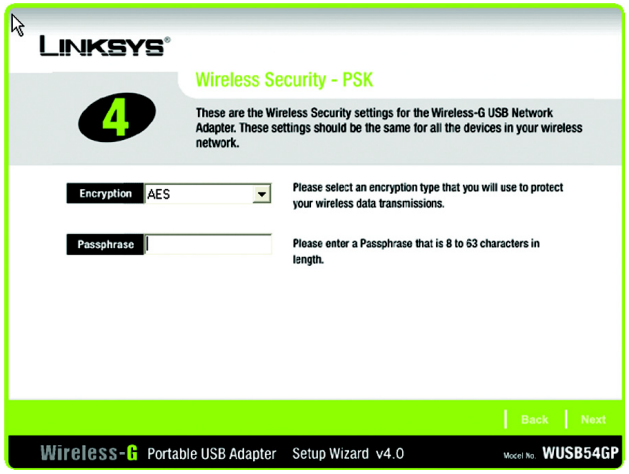
LINKSYS
Wireless Security - PSK
4
These are the Wireless Security settings for the Wireless-G USB Network Adapter. These settings should be the same for all the devices in your wireless network.
Encryption
AES
Please select an encryption type that you will use to protect your wireless data transmissions.
Passphrase
Please enter a Passphrase that is 8 to 63 characters in length.
Back
Next
Wireless-G Portable USB Adapter Setup Wizard v4.0
Model No. WUSB54GP

Figure 4-8: Setup Wizard's Wireless Security - PSK Using AES Screen

PSK + RADIUS

PSK + RADIUS features a Pre-Shared Key used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) PSK + RADIUS offers two encryption methods, TKIP and AES, with dynamic encryption keys, as well as two authentication methods, EAP-TLS and PEAP.

Authentication - Select the authentication method your network is using, **EAP-TLS** or **PEAP**.

EAP-TLS

If you selected EAP-TLS, enter the login name of your wireless network in the *Login Name* field. Enter the name of the authentication server in the *Server Name* field. From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network. Select the type of encryption, **TKIP** or **AES**, from the *Encryption* drop-down menu.

Click the **Next** button to continue. Click the **Back** button to return to the previous screen.

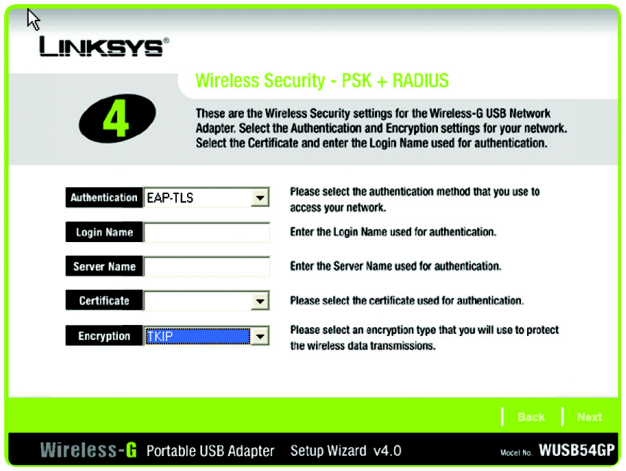
LINKSYS
Wireless Security - PSK + RADIUS
4
These are the Wireless Security settings for the Wireless-G USB Network Adapter. Select the Authentication and Encryption settings for your network. Select the Certificate and enter the Login Name used for authentication.
Authentication
EAP-TLS
Please select the authentication method that you use to access your network.
Login Name
Enter the Login Name used for authentication.
Server Name
Enter the Server Name used for authentication.
Certificate
Please select the certificate used for authentication.
Encryption
TKIP
Please select an encryption type that you will use to protect the wireless data transmissions.
Back
Next
Wireless-G Portable USB Adapter Setup Wizard v4.0
Model No. WUSB54GP

Figure 4-9: Setup Wizard's Wireless Security - PSK + RADIUS Using EAP-TLS Screen

PEAP

If you selected PEAP, enter the login name of your wireless network in the *Login Name* field. Enter the password of your wireless network in the *Password* field. Enter the name of the authentication server in the *Server Name* field. From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network. Select the type of encryption, **TKIP** or **AES**, from the *Encryption* drop-down menu.

Click the **Next** button to continue. Click the **Back** button to return to the previous screen.

LINKSYS
Wireless Security - PSK + RADIUS
4
These are the Wireless Security settings for the Wireless-G USB Network Adapter. Select the Authentication and Encryption settings for your network. Select the Certificate and enter the Login Name used for authentication.
Authentication
PEAP
Please select the authentication method that you use to access your network.
Login Name
Enter the Login Name used for authentication.
Password
Enter the Password used for authentication.
Server Name
Enter the Server Name used for authentication.
Certificate
Please select the certificate used for authentication.
Encryption
TKIP
Please select an encryption type that you will use to protect the wireless data transmissions.
Back
Next
Wireless-G Portable USB Adapter Setup Wizard v4.0
Model No. WUSB54GP

Figure 4-10: Setup Wizard's Wireless Security - PSK + RADIUS Using PEAP Screen

RADIUS

RADIUS features use of a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) RADIUS offers two authentication types: EAP-TLS and PEAP.

Authentication - Select the authentication method your network is using, **EAP-TLS** or **PEAP**.

EAP-TLS

If you selected EAP-TLS, enter the login name of your wireless network in the *Login Name* field. Enter the name of the authentication server in the *Server Name* field. From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network.

Click the **Next** button to continue. Click the **Back** button to return to the previous screen.

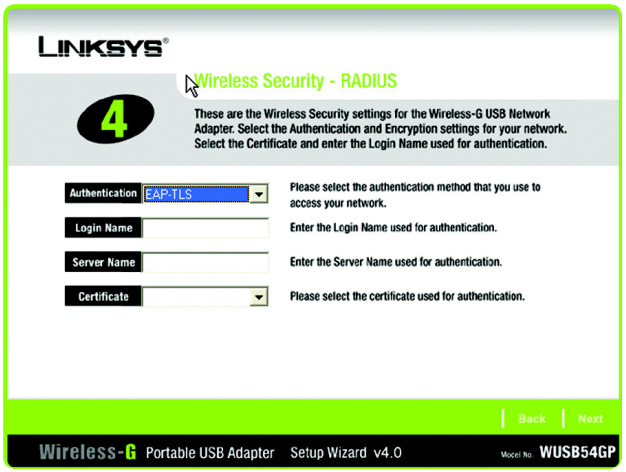
LINKSYS
Wireless Security - RADIUS
4
These are the Wireless Security settings for the Wireless-G USB Network Adapter. Select the Authentication and Encryption settings for your network. Select the Certificate and enter the Login Name used for authentication.
Authentication
EAP-TLS
Please select the authentication method that you use to access your network.
Login Name
Enter the Login Name used for authentication.
Server Name
Enter the Server Name used for authentication.
Certificate
Please select the certificate used for authentication.
Back
Next
Wireless-G Portable USB Adapter Setup Wizard v4.0
Model No. WUSB54GP

Figure 4-11: Setup Wizard's Wireless Security - RADIUS Using EAP-TLS Screen

PEAP

If you selected PEAP, enter the login name of your wireless network in the *Login Name* field. Enter the password of your wireless network in the *Password* field. Enter the name of the authentication server in the *Server Name* field. From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network.

Click the **Next** button to continue. Click the **Back** button to return to the previous screen.

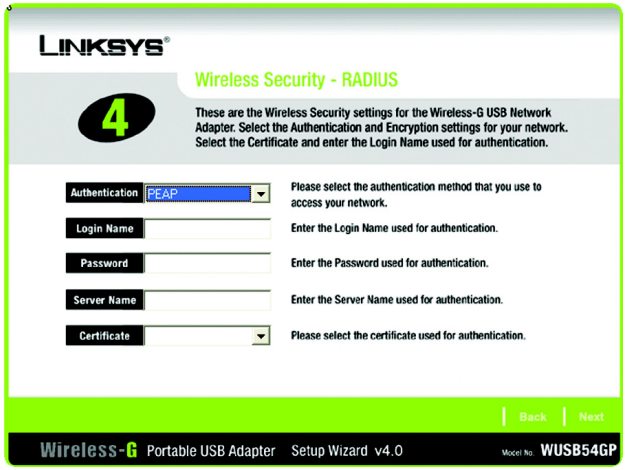
LINKSYS
Wireless Security - RADIUS
4
These are the Wireless Security settings for the Wireless-G USB Network Adapter. Select the Authentication and Encryption settings for your network. Select the Certificate and enter the Login Name used for authentication.
Authentication
PEAP
Please select the authentication method that you use to access your network.
Login Name
Enter the Login Name used for authentication.
Password
Enter the Password used for authentication.
Server Name
Enter the Server Name used for authentication.
Certificate
Please select the certificate used for authentication.
Back
Next
Wireless-G Portable USB Adapter Setup Wizard v4.0
Model No. WUSB54GP

Figure 4-12: Setup Wizard's Wireless Security - RADIUS Using PEAP Screen

7. The Setup Wizard will ask you to review your settings before it starts to install files. Click **Next** if you are satisfied with your settings, or click **Back** to change any settings.

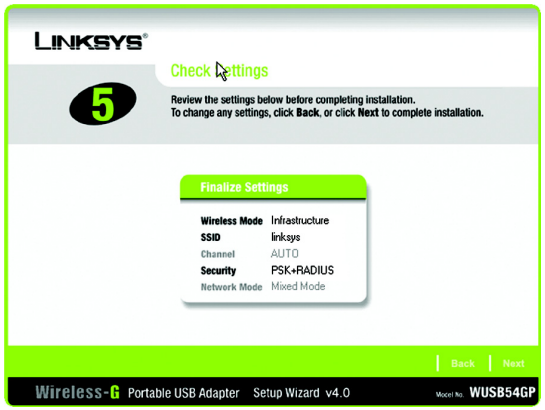

Figure 4-13: Setup Wizard's Check Settings Screen

8. At this point, you may see a *Digital Signature Not Found* screen indicating that a digital signature was not found. The Adapter's software has been tested and found to work successfully with Windows 2000. Click the **Yes** button to continue.

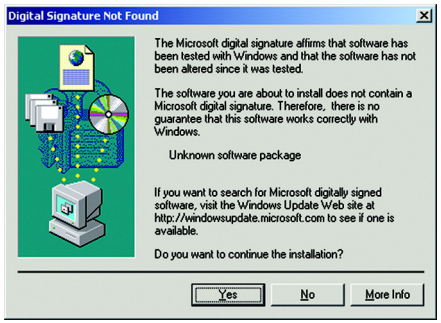
Digital Signature Not Found
The Microsoft digital signature affirms that software has been tested with Windows and that the software has not been altered since it was tested.
The software you are about to install does not contain a Microsoft digital signature. Therefore, there is no guarantee that this software works correctly with Windows.
Unknown software package
If you want to search for Microsoft digitally signed software, visit the Windows Update Web site at http://windowsupdate.microsoft.com to see if one is available.
Do you want to continue the installation?
Yes
No
More Info

Figure 4-14: Digital Signature Not Found Screen

NOTE: If you are using Windows 98 or Me, you may be asked to provide your original Windows CD to complete the installation. After successful installaton, you may also be required to restart your PC.

9. After the software has been successfully installed, the *Congratulations* screen will appear. Click the **Exit** button.

LINKSYS
A Division of Cisco Systems, Inc.
Congratulations
The installation of the Wireless-G Portable USB Adapter is complete.
2.4GHz 802.11g Wireless-G
Portable USB Adapter Setup Wizard ver. 4.0
Exit
WUSB54GP Copyright © 2004 Cisco Systems, Inc. All rights reserved.

Figure 4-15: Setup Wizard's Congratulations Screen

Proceed to "Chapter 5: Connecting the Wireless-G Portable USB Adapter."

Chapter 5: Connecting the Wireless-G Portable USB Adapter

IMPORTANT: You must run the Setup Wizard before connecting the Adapter to your computer.

1. To connect the Portable USB Adapter to your PC, simply plug the USB end into your PC's available USP port. Raise the antenna and adjust the Adapter so the antenna is perpendicular to the ground.

Figure 5-1: The Portable USB Adapter on Your Notebook

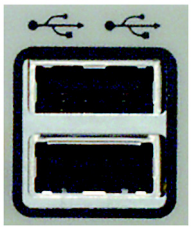

Figure 5-2: A USB Port

port: *the connection point on a computer or networking device used for plugging in a cable or an adapter.*

2. When Windows 2000 begins installing the Adapter's driver file, a screen stating that a digital signature was not found may appear. This software has been tested and found to work properly with Windows 2000. Click the **Yes** button to continue the installation.

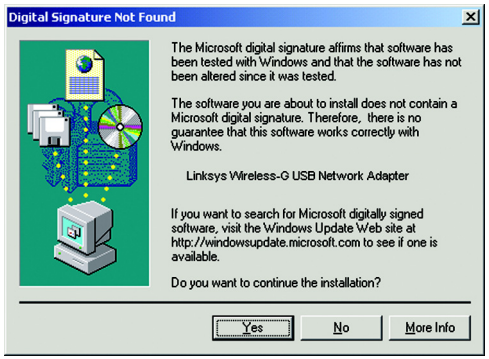
Digital Signature Not Found
The Microsoft digital signature affirms that software has been tested with Windows and that the software has not been altered since it was tested.
The software you are about to install does not contain a Microsoft digital signature. Therefore, there is no guarantee that this software works correctly with Windows.
Linksys Wireless-G USB Network Adapter
If you want to search for Microsoft digitally signed software, visit the Windows Update Web site at http://windowsupdate.microsoft.com to see if one is available.
Do you want to continue the installation?
Yes
No
More Info

Figure 5-3: Digital Signature Not Found Screen

The installation of the Wireless-G Portable USB Adapter is complete.

If you want to check the link information, search for available wireless networks, or make additional configuration changes, proceed to "Chapter 6: Using the Wireless Network Monitor."

Using the USB Extension Base

For better reception on the Portable USB Adapter, you can attach the USB Extension Base to your PC's USB port and connect the Portable USB Adapter to the USB Extension Base. Then, for better reception, you can more strategically place the USB Extension Base on a higher platform or away from interference.

Figure 5-4: Using the USB Extension Base

The installation of the Wireless-G Portable USB Adapter is complete.

If you want to check the link information, search for available wireless networks, or make additional configuration changes, proceed to "Chapter 6: Using the Wireless Network Monitor."

Using the Adapter's Wall Mount

The Adapter's Wall Mount allows you to easily attach the Adapter to your wall for better reception and more convenient placement.

1. Attach two screws to a wall at a distance of 1 1/2 inches apart.
2. Line up the mounting holes on the bottom of the Base with the screws, place the Base over the screws, and slide down into place.

The installation of the Wireless-G Adapter is complete.

If you want to check the link information, search for available wireless networks, or make additional configuration changes, go to "Chapter 6: Using the Wireless Network Monitor."

Figure 5-5: Using the Wall Mount

Chapter 6: Using the Wireless Network Monitor

Use the Wireless Network Monitor to check the link information, search for available wireless networks, or create profiles that hold different configuration settings.

Using the Wireless Network Monitor Icon

After installing the Adapter, the Wireless-G Portable USB Adapter Wireless Monitor icon will appear in your system tray. If the Wireless Network Monitor is enabled, then the icon will be green. If the Wireless Network Monitor is disabled or the Adapter is not connected, then the icon will be gray.

Figure 6-1: Wireless Network Monitor Icon

If you right-click the icon, you will see these choices:

- About - Click **About** to view the version information for the driver and Wireless Network Monitor.
- Use Windows XP Wireless Configuration (Windows XP only) - If your computer is running Windows XP, then this choice will be available. If you want to use Windows XP Wireless Zero Configuration to control the Adapter—instead of using the Wireless Network Monitor—then select **Use Windows XP Wireless Configuration**.

  If you want to switch back to the Wireless Network Monitor, right-click the **Wireless Network Monitor** icon, and select **Use Linksys Wireless Network Monitor**.

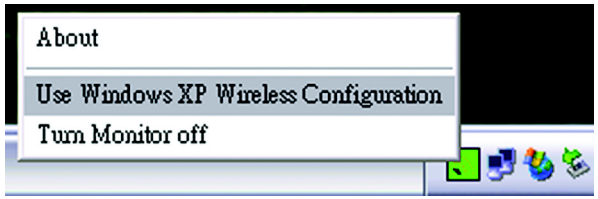

Figure 6-2: Windows XP - Use Windows XP Wireless Configuration

NOTE: For more information about Wireless Zero Configuration, refer to Windows Help.

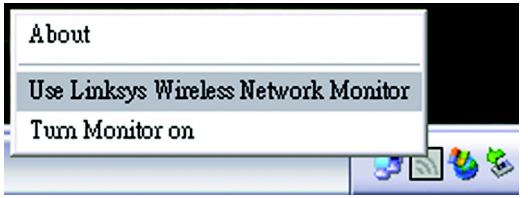

Figure 6-3: Windows XP - Use Linksys Wireless Network Monitor

- Turn Monitor on - Select **Turn Monitor on** to enable the Wireless Network Monitor.
- Turn Monitor off - Select **Turn Monitor off** to disable the Wireless Network Monitor.

Accessing the Wireless Network Monitor

Besides selecting *Turn on* when you right-click the icon, you can also double-click the **Wireless Network Monitor** icon to activate the Wireless Network Monitor. Then the *Link Information* screen will appear. From this screen, you can find out how strong the current wireless signal is and how good the connection's quality is. You can also click the **More Information** button to view additional status information about the current wireless connection. To search for available wireless networks, click the **Site Survey** tab. To perform configuration changes, click the **Profiles** tab.

Link Information

The *Link Information* screen displays network mode, signal strength, and link quality information about the current connection. It also provides a button to click for additional status information.

Ad-Hoc Mode or **Infrastructure Mode** - The screen indicates whether the Adapter is currently working in ad-hoc or infrastructure mode.

Signal Strength - The Signal Strength bar indicates signal strength.

Link Quality - The Link Quality bar indicates the quality of the wireless network connection.

Click the **More Information** button to view additional information about the wireless network connection.

Clicking the **More Information** button displays the *Wireless Network Status* screen, which displays more information about the Adapter's connection.

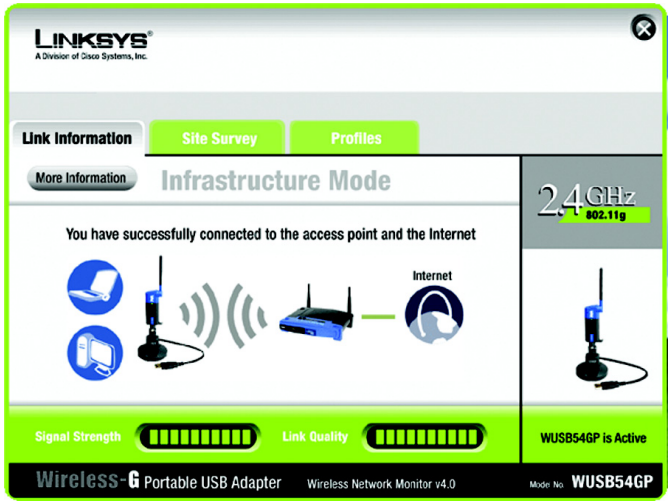

Figure 6-4: Link Information

Wireless Network Status

The *Wireless Network Status* screen provides information on your current network settings.

Status - The status of the wireless network connection.

SSID - This is the unique name of the wireless network.

Wireless Mode - The mode of the wireless network currently in use is displayed here.

Transfer Rate - The data transfer rate of the current connection is shown here.

Channel - This is the channel to which the wireless network devices are set.

Security - The status of the wireless security feature is displayed here.

Authentication - This is your wireless network's authentication method.

IP Address - The IP Address of the Adapter is displayed here.

Subnet Mask - The Subnet Mask of the Adapter is shown here.

Default Gateway - The Default Gateway address of the Adapter is displayed here.

DNS - This is the DNS address of the Adapter.

DHCP Client - This displays the Adapter's status as a DHCP client.

MAC - The MAC address of the wireless network's access point is shown here.

Signal Strength - The Signal Strength bar indicates the signal strength.

Link Quality - The Link Quality bar indicates the quality of the wireless network connection.

Click the **Statistics** button to go to the *Wireless Network Statistics* screen. Click the **Back** button to return to the initial *Link Information* screen. Click the **Save to Profile** button to save the currently active connection settings to a profile.

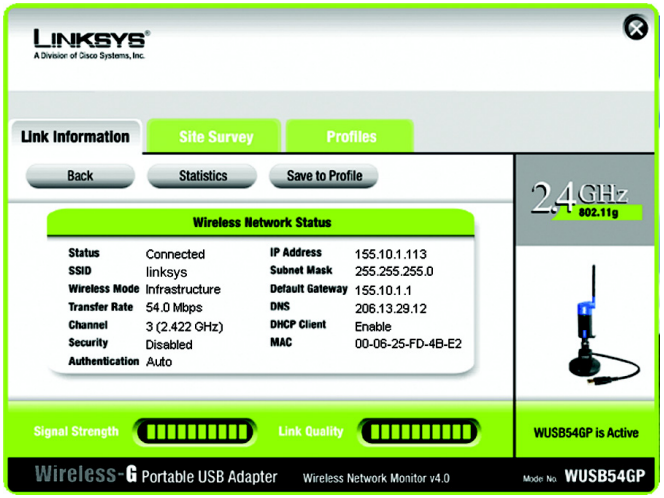

Figure 6-5: More Information - Wireless Network Status

Wireless Network Statistics

The *Wireless Networks Statistics* screen provides statistics on your current network settings.

Transmit Rate - This is the data transfer rate of the current connection. (In Auto mode, the Adapter dynamically shifts to the fastest data transfer rate possible at any given time.)

Receive Rate - This is the rate at which data is received.

Packets Received - This shows the packets received by the Adapter, in real time, since connecting to the Wireless Network or since the *Refresh Statistics* button was last pressed.

Packets Transmitted - This shows the packets transmitted from the Adapter, in real time, since connecting to the Wireless Network or since the *Refresh Statistics* button was last pressed.

Bytes Received - This shows the bytes received by the Adapter, in real time, since connecting to the Wireless Network or since the *Refresh Statistics* button was last pressed.

Bytes Transmitted - This shows the bytes transmitted from the Adapter, in real time, since connecting to the Wireless Network or since the *Refresh Statistics* button was last pressed.

Noise Level - This shows the level of background noise affecting the wireless signal. A lower reading translates into a higher quality signal.

Signal Strength - This is the intensity of the wireless signal received by the Adapter.

Up Time - This indicates the length of the most recent connection to a wireless network.

Total Up Time - This indicates the cumulative total of the Adapter's connection time.

Driver Version - This shows the version of the Adapter's driver.

Signal Strength - The Signal Strength bar indicates the signal strength.

Link Quality - The Link Quality bar indicates the quality of the wireless network connection.

Click the **Back** button to return to the initial *Link Information* screen. Click the **Status** button to go to the *Wireless Network Status* screen. Click the **Save to Profile** button to save the currently active connection settings to a profile. Click the **Refresh Statistics** button to update or reset the statistics. The Wireless Network Monitor will update the Transmit Rate, Receive Rate, Noise Level, and Signal Strength statistics. At the same time, the Packets Received and Transmitted counts, Bytes Received and Transmitted counts, and Up Time statistic will be reset to zero. (The Total Up Time statistic will not be reset.)

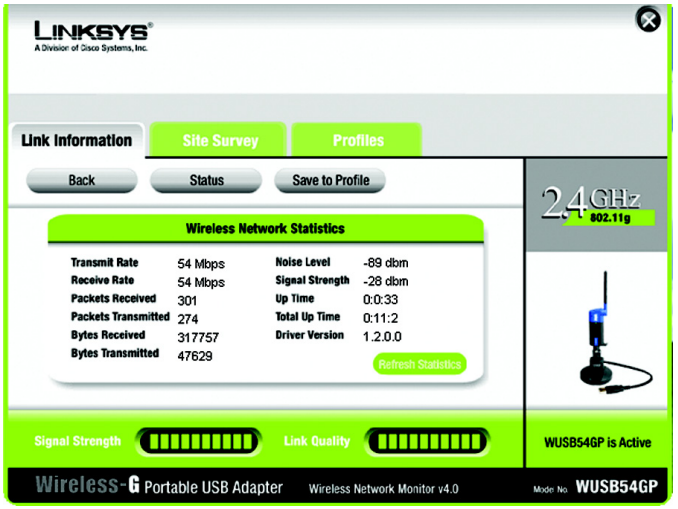

Figure 6-6: More Information-Network Statistics

Site Survey

The *Site Survey* screen displays a list of infrastructure and ad-hoc networks available for connection in the table on the left. This table shows the network's SSID, Channel, and the quality of the wireless signal the Adapter is receiving. You may click **SSID**, **CH (Channel)**, or **Signal**, to sort by that field.

SSID - The SSID or unique name of the wireless network is displayed here.

CH - This is the channel setting that the network uses.

Signal - This is the percentage of signal strength, from 0 to 100%.

Site Information

For each network selected, the following settings are listed:

SSID - This the SSID or unique name of the wireless network.

Wireless Mode - This is the mode of the wireless network currently in use.

Channel - This is the channel to which the wireless network devices are set.

Security - The status of the wireless security feature is displayed here.

MAC - The MAC address of the wireless network's access point is displayed here.

Refresh - Click the **Refresh** button to perform a new search for wireless devices.

Connect - To connect to one of the networks on the list, select the wireless network, and click the **Connect** button. If the network has encryption enabled, then you will see a new screen appear.

From the *Security* drop-down menu, select the network's encryption method, **WEP** or **PSK**.

If you selected WEP, then you will see the *WEP Key Needed for Connection* screen. Select the appropriate level of WEP encryption, **64-bit** or **128-bit**. Then enter the network's Passphrase or WEP Key. Click the **Connect** button. To cancel the connection, click the **Cancel** button.

If you selected PSK, then you will see the *PSK (Pre-Shared Key) Needed for Connection* screen. Select the appropriate encryption type, **TKIP** or **AES**. Then enter the network's Passphrase or Pre-Shared Key in the *Passphrase* field. Then click the **Connect** button. To cancel the connection, click the **Cancel** button.

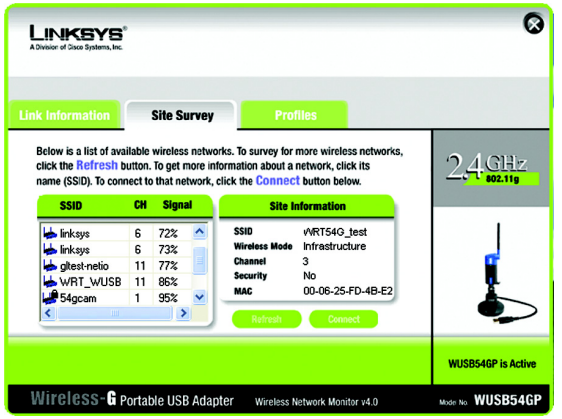

Figure 6-7: Site Survey

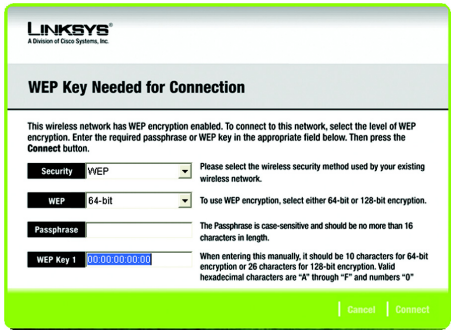
LINKSYS
A Division of Cisco Systems, Inc.
WEP Key Needed for Connection
This wireless network has WEP encryption enabled. To connect to this network, select the level of WEP encryption. Enter the required passphrase or WEP key in the appropriate field below. Then press the Connect button.
Security WEP
Please select the wireless security method used by your existing wireless network.
WEP 64-bit
To use WEP encryption, select either 64-bit or 128-bit encryption.
Passphrase
The Passphrase is case-sensitive and should be no more than 16 characters in length.
WEP Key 1 00:00:00:00:00
When entering this manually, it should be 10 characters for 64-bit encryption or 26 characters for 128-bit encryption. Valid hexadecimal characters are "A" through "F" and numbers "0"
Cancel
Connect

Figure 6-8: WEP Key Needed for Connection

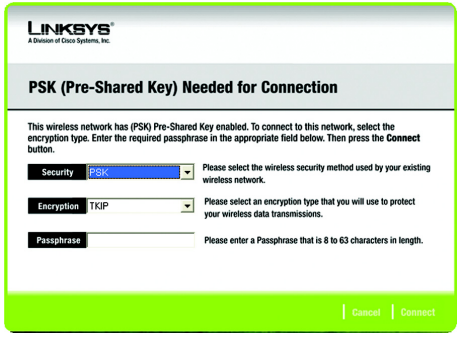
LINKSYS
A Division of Cisco Systems, Inc.
PSK (Pre-Shared Key) Needed for Connection
This wireless network has (PSK) Pre-Shared Key enabled. To connect to this network, select the encryption type. Enter the required passphrase in the appropriate field below. Then press the Connect button.
Security PSK
Please select the wireless security method used by your existing wireless network.
Encryption TKIP
Please select an encryption type that you will use to protect your wireless data transmissions.
Passphrase
Please enter a Passphrase that is 8 to 63 characters in length.
Cancel
Connect

Figure 6-9: PSK (Pre-Shared Key) Needed for Connection

Profiles

The *Profiles* screen lets you save different configuration profiles for different network setups. The table on the left displays a list of infrastructure and ad-hoc networks available for connection. This table shows the network's profile name and the wireless network's SSID, as set in the connection profile.

Profile Information

For each profile selected, the following are listed:

Wireless Mode - This is the mode of the wireless network currently in use.

Transfer Rate - The Adapter is set to Auto mode, so it will dynamically shift to the fastest data transfer rate possible at any given time.

Channel - This is the channel to which the wireless network devices are set.

Security - The status of the wireless security feature is displayed here.

Authentication - The authentication setting for the network is shown here.

Connect - To connect to a wireless network using a specific profile, select the profile, and click the **Connect** button.

New - Click the **New** button to create a new profile. See the next section, "Creating a New Profile," for detailed instructions.

Edit - Select a profile, and click the **Edit** button to change an existing profile.

Import - Click the **Import** button to import a profile that has been saved in another location. Select the appropriate file, and click the **Open** button.

Export - Select the profile you want to save in a different location, and click the **Export** button. Direct Windows to the appropriate folder, and click the **OK** button.

Delete - Click the **Delete** button to delete a profile.

NOTE: If you want to export more than one profile, you have to export them one at a time.

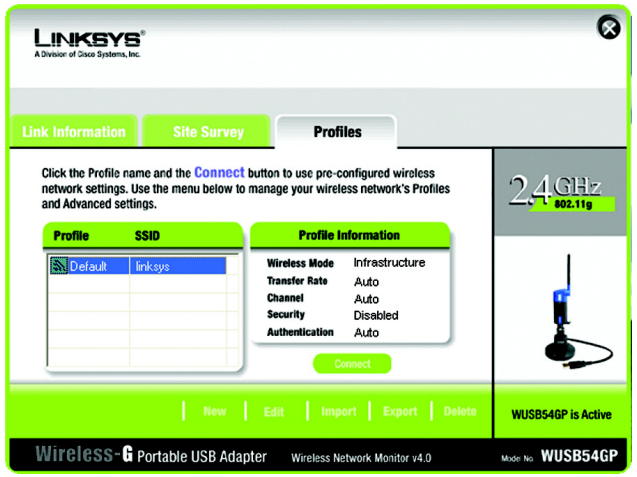

Figure 6-10: Profiles

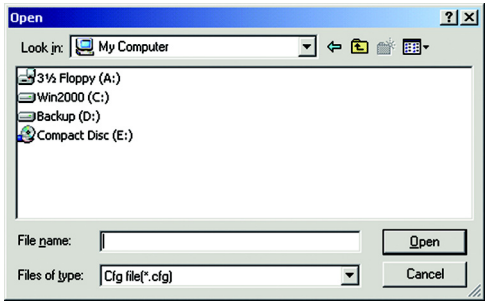

Figure 6-11: Import a Profile

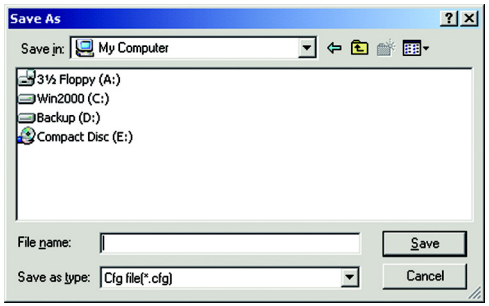

Figure 6-12: Export a Profile

Creating a New Profile

1. On the *Profiles* screen, click the **New** button to create a new profile.

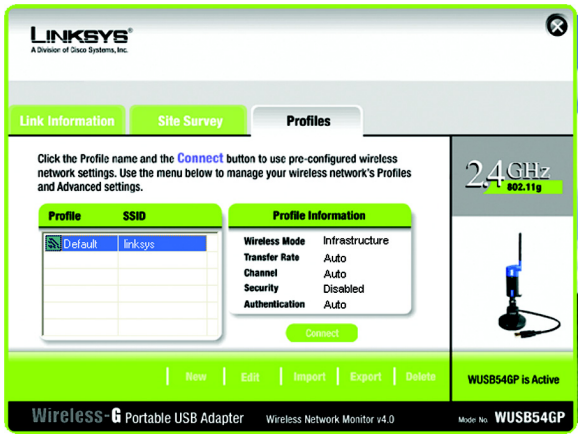

Figure 6-13: Create a New Profile

2. Enter a name for the new profile, and click the **OK** button. Click the **Cancel** button to return to the *Profiles* screen without entering a name.

Figure 6-14: Enter Profile Name

3. The *Network Settings* screen will appear. If your network has a router or other DHCP server, click the radio button next to **Obtain network settings automatically (DHCP)**. Click the **Next** button to continue, or click the **Cancel** button to return to the *Profiles* screen.

   If your network does not have a DHCP server, click the radio button next to **Specify the network settings**. Enter an IP Address, Subnet Mask, Default Gateway, and DNS address appropriate for your network. You must specify the IP Address and Subnet Mask on this screen. If you are unsure about the Default Gateway and DNS address, leave these fields empty. Click the **Next** button to continue, or click the **Cancel** button to return to the *Profiles* screen.

   IP Address - This IP Address must be unique to your network.

   Subnet Mask - The Adapter's Subnet Mask must be the same as your wired network's Subnet Mask.

   Default Gateway - Enter the IP address of your network's Gateway here.

   DNS 1 and **DNS 2** - Enter the DNS address of your wired Ethernet network here.

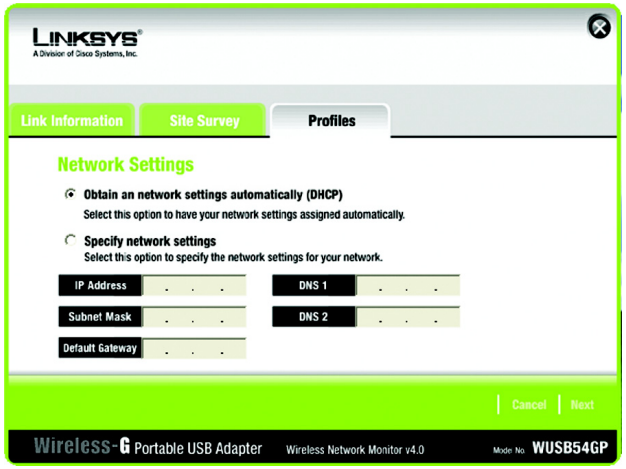

Figure 6-15: Network Settings for New Profile

4. The *Wireless Mode* screen shows a choice of two wireless modes. Click the **Infrastructure Mode** radio button if you want your wireless computers to communicate with computers on your wired network via a wireless access point. Click the **Ad-Hoc Mode** radio button if you want multiple wireless computers to communicate directly with each other. Enter the SSID for your network.

   Click the **Next** button to continue or the **Back** button to return to the previous screen.

   Infrastructure Mode - This mode allows wireless and wired networks to communicate through an access point.

   Ad-Hoc Mode - This mode allows wireless-equipped computers to communicate directly with each other. No access point is used.

   SSID - This is the network name. It must be used for all the devices in your wireless network. It is case-sensitive. It should be a unique name to help prevent others from entering your network.

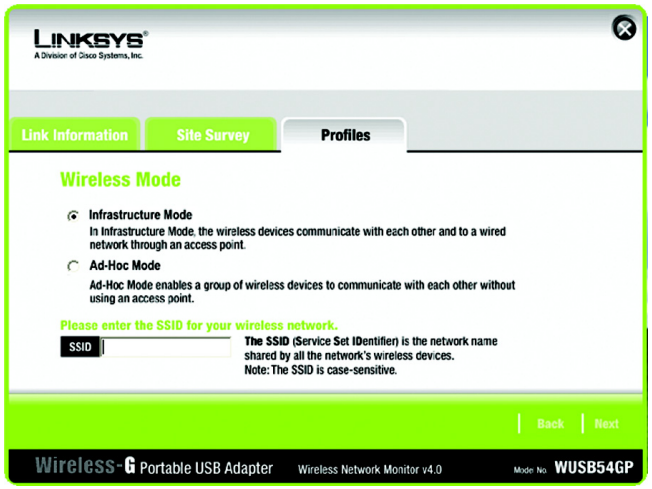
LINKSYS
A Division of Cisco Systems, Inc.
Link Information
Site Survey
Profiles
Wireless Mode
Infrastructure Mode
In Infrastructure Mode, the wireless devices communicate with each other and to a wired network through an access point.
Ad-Hoc Mode
Ad-Hoc Mode enables a group of wireless devices to communicate with each other without using an access point.
Please enter the SSID for your wireless network.
SSID
The SSID (Service Set IDentifier) is the network name shared by all the network's wireless devices.
Note: The SSID is case-sensitive.
Back
Next
Wireless-G Portable USB Adapter
Wireless Network Monitor v4.0
Mode No. WUSB54GP

Figure 6-16: Wireless Mode for New Profile

5. The *Ad-Hoc Mode Settings* screen will appear. If you chose Infrastructure Mode, go to Step 6 now. If you chose Ad-Hoc Mode, select the correct operating channel for your network from the *Channel* drop-down menu. Then, select the Network Mode from the drop-down menu. Click the **Next** button, and go to Step 6. Click the **Back** button to change any settings.

   Channel - The channel you choose should match the channel set on the other devices in your wireless network. If you are unsure about which channel to use, select the default channel (Channel 6).

   Network Mode - Select **Mixed Mode**, and both Wireless-G and Wireless-B computers will be allowed on the network, but the speed may be reduced. Select **G-Only Mode** for maximum speed, but no Wireless-B users will be allowed on the network.

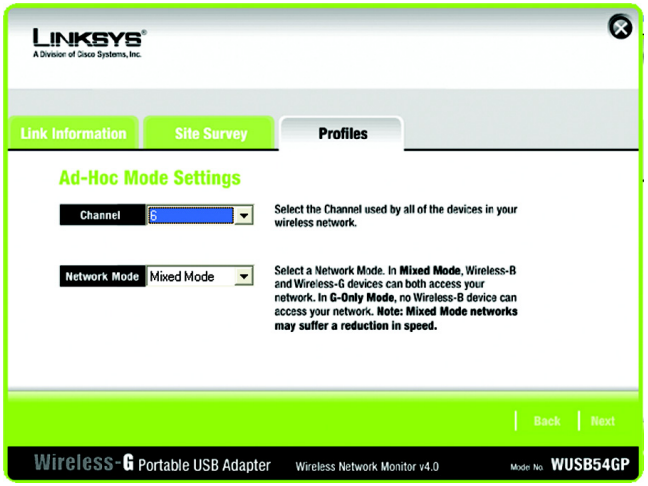
LINKSYS
A Division of Cisco Systems, Inc.
Link Information
Site Survey
Profiles
Ad-Hoc Mode Settings
Channel
6
Select the Channel used by all of the devices in your wireless network.
Network Mode
Mixed Mode
Select a Network Mode. In Mixed Mode, Wireless-B and Wireless-G devices can both access your network. In G-Only Mode, no Wireless-B device can access your network. Note: Mixed Mode networks may suffer a reduction in speed.
Back
Next
Wireless-G Portable USB Adapter
Wireless Network Monitor v4.0
Mode No. WUSB54GP

Figure 6-17: Ad-Hoc Mode Settings for New Profile

6. Select the method of security you want to use: **WEP**, **PSK**, **PSK + RADIUS**, or **RADIUS**. WEP stands for Wired Equivalent Privacy, and PSK stands for Pre-Shared Key. RADIUS stands for Remote Authentication Dial-In User Service.

NOTE: If your network is using WPA-Personal or WPA-PSK security, then select **PSK**. If your network is using WPA-Enterprise or WPA-RADIUS security, then select **PSK + RADIUS**.

If you don't want to use encryption, select **Disabled** and then click the **Next** button to continue. Proceed to Step 8.

Click the **Next** button to continue or the **Back** button to return to the previous screen.

7. Proceed to the appropriate section for your security method: WEP, PSK, PSK-RADIUS, or RADIUS.

WEP

WEP - Select **64-bit** or **128-bit** encryption from the drop-down menu, and enter a passphrase or WEP key.

Passphrase - Enter a passphrase in the *Passphrase* field, so a WEP key is automatically generated. It is case-sensitive and should not be longer than 16 alphanumeric characters. This passphrase must match the passphrase of your other wireless network devices and is compatible with Linksys wireless products only. (If you have any non-Linksys wireless products, enter the WEP key manually on those products.)

WEP Key - The WEP key you enter must match the WEP key of your wireless network. For 64-bit encryption, enter exactly 10 hexadecimal characters. For 128-bit encryption, enter exactly 26 hexadecimal characters. Valid hexadecimal characters are "0" to "9" and "A" to "F".

Advanced Users
TX Key - The default transmit key number is 1. If your network's access point or wireless router uses transmit key number 2, 3, or 4, select the appropriate number from the *TX Key* drop-down box.

Authentication -The default is set to **Auto**, so it will auto-detect for **Shared Key** or **Open System** authentication. For Shared Key authentication, both the sender and the recipient share a WEP key for authentication. For Open System authentication, the sender and the recipient do not share a WEP key for authentication. If you are not sure which authentication method to select, keep the default, **Auto**.

Click the **Next** button to continue. Click the **Back** button to return to the previous screen.

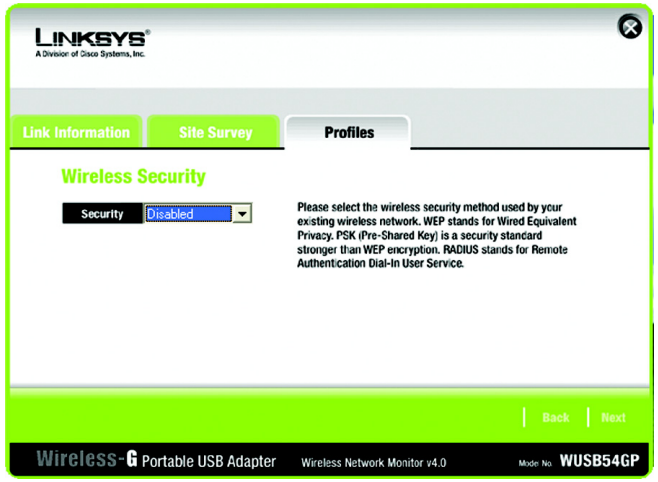
LINKSYS
A Division of Cisco Systems, Inc.
Link Information
Site Survey
Profiles
Wireless Security
Security
Disabled
Please select the wireless security method used by your existing wireless network. WEP stands for Wired Equivalent Privacy. PSK (Pre-Shared Key) is a security standard stronger than WEP encryption. RADIUS stands for Remote Authentication Dial-In User Service.
Back
Next
Wireless-G Portable USB Adapter
Wireless Network Monitor v4.0
Model No. WUSB54GP

Figure 6-18: Wireless Security for New Profile

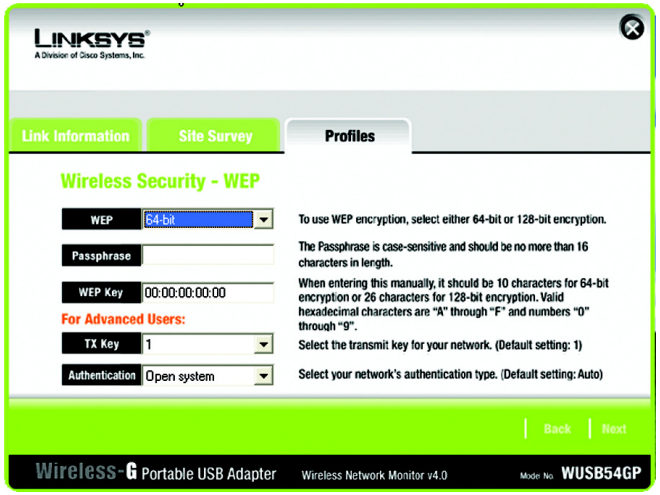
LINKSYS
A Division of Cisco Systems, Inc.
Link Information
Site Survey
Profiles
Wireless Security - WEP
WEP
64-bit
To use WEP encryption, select either 64-bit or 128-bit encryption.
Passphrase
The Passphrase is case-sensitive and should be no more than 16 characters in length.
WEP Key
00:00:00:00:00
When entering this manually, it should be 10 characters for 64-bit encryption or 26 characters for 128-bit encryption. Valid hexadecimal characters are "A" through "F" and numbers "0" through "9".
For Advanced Users:
TX Key
1
Select the transmit key for your network. (Default setting: 1)
Authentication
Open system
Select your network's authentication type. (Default setting: Auto)
Back
Next
Wireless-G Portable USB Adapter
Wireless Network Monitor v4.0
Model No. WUSB54GP

Figure 6-19: Wireless Security - WEP for New Profile

PSK

PSK offers two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **TKIP** or **AES**, for the *Encryption Type*. Then enter a Passphrase that is 8-63 characters in length.

Encryption - Select the type of algorithm you want to use, **TKIP** or **AES**, for the *Encryption Type*.

Passphrase - Enter a Passphrase, also called a Pre-Shared Key, of 8-63 characters in the *Passphrase* field. The longer and more complex your Passphrase is, the more secure your network will be.

Click the **Next** button to continue. Click the **Back** button to return to the previous screen.

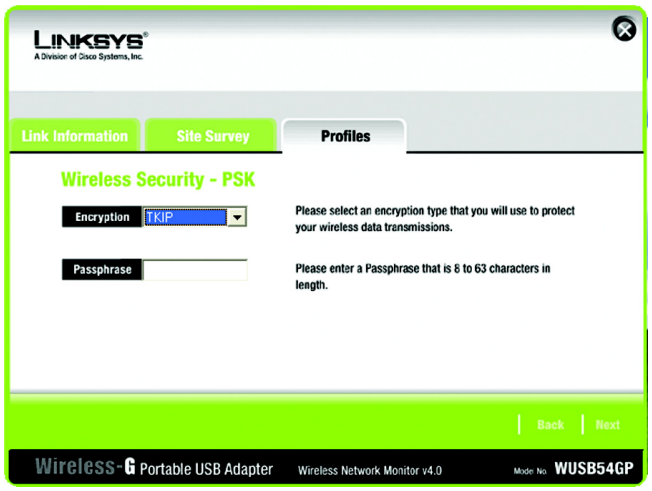

Figure 6-20: Wireless Security - PSK for New Profile

PSK + RADIUS

PSK + RADIUS features a Pre-Shared Key used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) PSK + RADIUS offers two encryption methods, TKIP and AES, with dynamic encryption keys, as well as two authentication methods, EAP-TLS and PEAP.

Authentication - Select the authentication method your network is using, **EAP-TLS** or **PEAP**.

EAP-TLS

If you selected EAP-TLS, enter the login name of your wireless network in the *Login Name* field. Enter the name of the authentication server in the *Server Name* field. From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network. Select the type of encryption, **TKIP** or **AES**, for the *Encryption* field.

Click the **Next** button to continue. Click the **Back** button to return to the previous screen.

PEAP

If you selected PEAP, enter the login name of your wireless network in the *Login Name* field. Enter the password of your wireless network in the *Password* field. Enter the name of the authentication server in the *Server Name* field. From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network. Select the type of encryption, **TKIP** or **AES**, for the *Encryption* field.

Click the **Next** button to continue. Click the **Back** button to return to the previous screen.

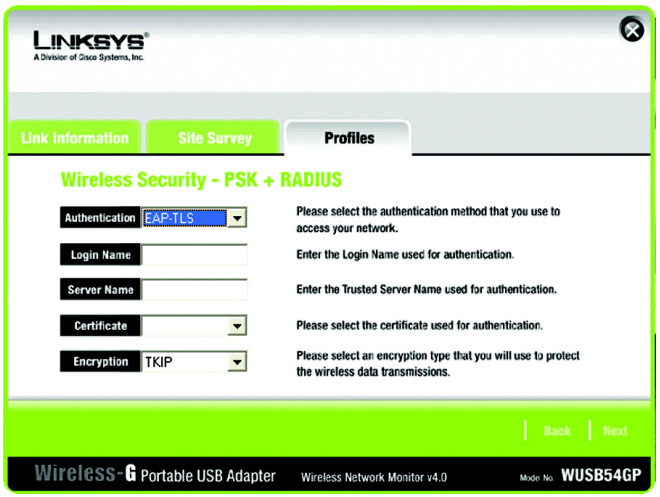

Figure 6-21: Wireless Security - PSK + RADIUS Using EAP-TLS for New Profile

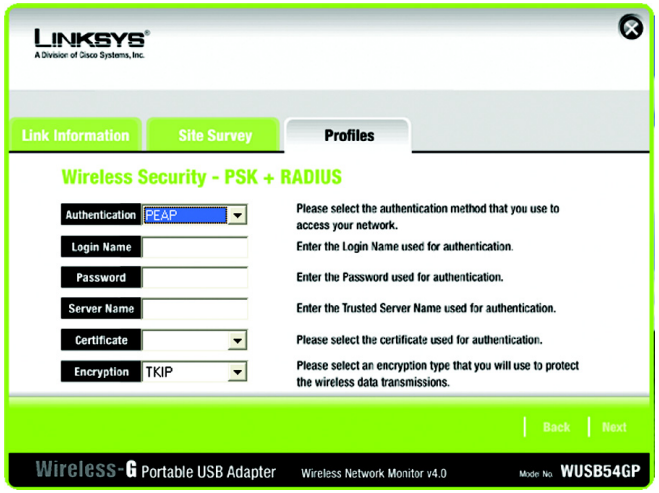

Figure 6-22: Wireless Security - PSK + RADIUS Using PEAP for New Profile

RADIUS

RADIUS features use of a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) RADIUS offers two authentication types: EAP-TLS and PEAP.

Authentication - Select the authentication method your network is using, **EAP-TLS** or **PEAP**.

EAP-TLS

If you selected EAP-TLS, enter the login name of your wireless network in the *Login Name* field. Enter the name of the authentication server in the *Server Name* field. From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network.

Click the **Next** button to continue. Click the **Back** button to return to the previous screen.

PEAP

If you selected PEAP, enter the login name of your wireless network in the *Login Name* field. Enter the password of your wireless network in the *Password* field. Enter the name of the authentication server in the *Server Name* field. From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network.

Click the **Next** button to continue. Click the **Back** button to return to the previous screen.

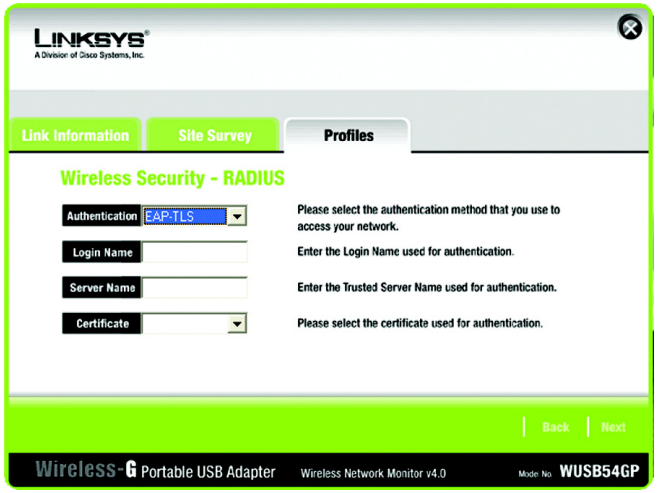

Figure 6-23: Wireless Security - RADIUS Using EAP-TLS for New Profile

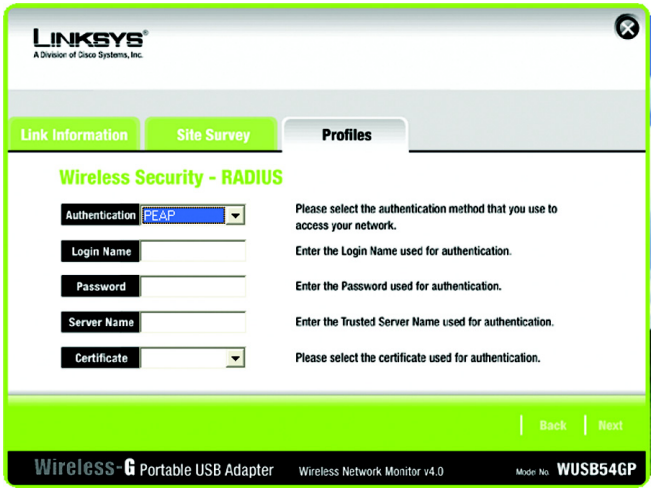

Figure 6-24: Wireless Security - RADIUS Using PEAP for New Profile

8. The *Confirm New Settings* screen will appear next and show the new settings. To save the new settings, click the **Save** button. To edit the new settings, click the **Back** button. To exit the Wireless Network Monitor, click **Exit**.

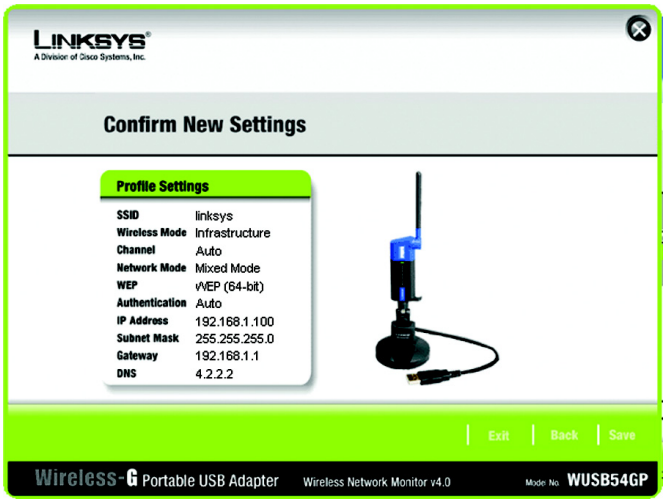

Figure 6-25: Confirm New Settings for New Profile

9. The *Congratulations* screen will appear next. Click **Connect to Network** to implement the new settings immediately and return to the *Link Information* screen. Click **Return to Profiles Screen** to keep the current settings active and return to the *Profiles* screen.

You have successfully created a connection profile.

Figure 6-26: Congratulations for New Profile

Appendix A: Troubleshooting

This appendix consists of two parts: “Common Problems and Solutions” and “Frequently Asked Questions.” This appendix provides solutions to problems that may occur during the installation and operation of the Wireless-G Portable USB Adapter. Read the description below to solve your problems. If you can't find an answer here, check the Linksys website at *www.linksys.com*.

Common Problems and Solutions

1. ***My computer does not recognize the Wireless-G Portable USB Adapter.***
   Follow the steps below until the problem is solved:
   - Make sure the Adapter is properly connected to the PC’s USB port.
   - Make sure that the USB Controller is enabled in the BIOS. Refer to the documentation for your PC’s motherboard.

2. ***The Wireless-G Portable USB Adapter does not work properly.***
   Follow the steps below until the problem is solved:
   - Reinsert the Wireless-G Portable USB Adapter into the notebook or desktop’s USB port.
   - Click **Start** and select **Settings**. Click **Control Panel**. Double-click **System**. Click the **Hardware** tab. Click the **Device Manager** button. You will find the Wireless-G Portable USB Adapter if it is installed successfully. If not, disconnect the Adapter and uninstall the driver software from your PC. Then restart your PC and repeat the software and hardware installation specified in this User Guide.

3. ***I cannot communicate with the other computers linked via Ethernet in the Infrastructure configuration.***
   Follow the steps below until the problem is solved:
   - Make sure that the notebook or desktop PC is powered on.
   - Make sure that the Wireless-G Portable USB Adapter is configured with the same SSID and security settings as the other computers in the Infrastructure configuration.

Frequently Asked Questions

Can I run an application from a remote computer over the wireless network?
This will depend on whether or not the application is designed to be used over a network. Consult the application's user guide to determine if it supports operation over a network.

Can I play computer games with other members of the wireless network?
Yes, as long as the game supports multiple players over a LAN (local area network). Refer to the game's user guide for more information.

What is the IEEE 802.11b standard?
It is one of the IEEE standards for wireless networks. The 802.11b standard allows wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11b standard. The 802.11b standard states a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz.

What is the IEEE 802.11g standard?
It is one of the IEEE standards for wireless networks. The 802.11g standard allows wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11g standard. The 802.11g standard states a maximum data transfer rate of 54Mbps and an operating frequency of 2.4GHz.

What IEEE 802.11b features are supported?
The product supports the following IEEE 802.11b functions:

- CSMA/CA plus Acknowledge protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation
- Power Management

What IEEE 802.11g features are supported?
The product supports the following IEEE 802.11g functions:

- CSMA/CA plus Acknowledge protocol
- OFDM protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation
- Power Management

mbps: *one million bits per second; a unit of measurement for data transmission.*

fragmentation: *breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.*

What is ad-hoc mode?

When a wireless network is set to ad-hoc mode, the wireless-equipped computers are configured to communicate directly with each other. The ad-hoc wireless network will not communicate with any wired network.

What is infrastructure mode?

When a wireless network is set to infrastructure mode, the wireless network is configured to communicate with a wired network through a wireless access point.

What is roaming?

Roaming is the ability of a portable computer user to communicate continuously while moving freely throughout an area greater than that covered by a single access point. Before using the roaming function, the workstation must make sure that it is the same channel number with the access point of dedicated coverage area.

To achieve true seamless connectivity, the wireless LAN must incorporate a number of different functions. Each node and access point, for example, must always acknowledge receipt of each message. Each node must maintain contact with the wireless network even when not actually transmitting data. Achieving these functions simultaneously requires a dynamic RF networking technology that links access points and nodes. In such a system, the user's end node undertakes a search for the best possible access to the system. First, it evaluates such factors as signal strength and quality, as well as the message load currently being carried by each access point and the distance of each access point to the wired backbone. Based on that information, the node next selects the right access point and registers its address. Communications between end node and host computer can then be transmitted up and down the backbone.

ism band: *radio bandwidth utilized in wireless transmissions.*

spread spectrum: *wideband radio frequency technique used for more reliable and secure data transmission.*

dsss: *Frequency transmission with a redundant bit pattern resulting in a lower probability of information being lost in transit.*

As the user moves on, the end node's RF transmitter regularly checks the system to determine whether it is in touch with the original access point or whether it should seek a new one. When a node no longer receives acknowledgment from its original access point, it undertakes a new search. Upon finding a new access point, it then re-registers, and the communication process continues.

What is ISM band?

The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4 GHz, in particular, is being made available worldwide. This presents a truly revolutionary opportunity to place convenient high-speed wireless capabilities in the hands of users around the globe.

What is Spread Spectrum?

Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade-off produces a signal that is, in effect, louder and thus easier to detect, provided that

the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

What is DSSS? What is FHSS? And what are their differences?

Frequency-Hopping Spread-Spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct-Sequence Spread-Spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

Would the information be intercepted while transmitting on air?

WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, WLAN offers the encryption function (WEP) to enhance security and access control.

What is WEP?

WEP is Wired Equivalent Privacy, a data privacy mechanism based on a shared key algorithm, as described in the IEEE 802.11 standard. For more information, refer to “Appendix B: Wireless Security.”

What is WPA?

WPA is Wi-Fi Protected Access, a wireless security protocol that can be used in conjunction with a RADIUS server. For more information, refer to “Appendix B: Wireless Security.”

What is RADIUS?

RADIUS is Remote Authentication Dial-In User Service, which uses an authentication server to control network access. For more information, refer to “Appendix B: Wireless Security.”

Appendix B: Wireless Security

Linksys wants to make wireless networking as safe and easy for you as possible. The current generation of Linksys products provide several network security features, but they require specific action on your part for implementation. So, keep the following in mind whenever you are setting up or using your wireless network.

Security Precautions

The following is a complete list of security precautions to take (as shown in this User Guide) (at least steps 1 through 5 should be followed):

1. Change the default SSID.
2. Disable SSID Broadcast.
3. Change the default password for the Administrator account.
4. Enable MAC Address Filtering.
5. Change the SSID periodically.
6. Use the highest encryption algorithm possible. Use WPA if it is available. Please note that this may reduce your network performance.
7. Change the WEP encryption keys periodically.

To ensure network security, steps one through five should be followed, at least.

Note: Some of these security features are available only through the network router or access point. Refer to the router or access point's documentation for more information.

Security Threats Facing Wireless Networks

Wireless networks are easy to find. Hackers know that in order to join a wireless network, wireless networking products first listen for "beacon messages". These messages can be easily decrypted and contain much of the network's information, such as the network's SSID (Service Set Identifier). Here are the steps you can take:

Change the administrator's password regularly. With every wireless networking device you use, keep in mind that network settings (SSID, WEP keys, etc.) are stored in its firmware. Your network administrator is the only person who can change network settings. If a hacker gets a hold of the administrator's password, he, too, can change those settings. So, make it harder for a hacker to get that information. Change the administrator's password regularly.

SSID. There are several things to keep in mind about the SSID:

1. Disable Broadcast

2. Make it unique

3. Change it often

Most wireless networking devices will give you the option of broadcasting the SSID. While this option may be more convenient, it allows anyone to log into your wireless network. This includes hackers. So, don't broadcast the SSID.

Wireless networking products come with a default SSID set by the factory. (The Linksys default SSID is "linksys".) Hackers know these defaults and can check these against your network. Change your SSID to something unique and not something related to your company or the networking products you use.

Change your SSID regularly so that any hackers who have gained access to your wireless network will have to start from the beginning in trying to break in.

MAC Addresses. Enable MAC Address filtering. MAC Address filtering will allow you to provide access to only those wireless nodes with certain MAC Addresses. This makes it harder for a hacker to access your network with a random MAC Address.

WEP Encryption. Wired Equivalent Privacy (WEP) is often looked upon as a cure-all for wireless security concerns. This is overstating WEP's ability. Again, this can only provide enough security to make a hacker's job more difficult.

There are several ways that WEP can be maximized:

1. Use the highest level of encryption possible

2. Use "Shared Key" authentication

3. Change your WEP key regularly

WPA. Wi-Fi Protected Access (WPA) is the newest and best available standard in Wi-Fi security. Two modes are available: Pre-Shared Key and RADIUS. Pre-Shared Key gives you a choice of two encryption methods: TKIP (Temporal Key Integrity Protocol), which utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers, and AES (Advanced Encryption System), which utilizes a symmetric 128-Bit block data encryption. RADIUS (Remote Authentication Dial-In User Service) utilizes a RADIUS server for authentication and the use of dynamic TKIP, AES, or WEP.

Important: Always remember that each device in your wireless network MUST use the same encryption method and encryption key or your wireless network will not function properly.

WPA Pre-Shared Key. If you do not have a RADIUS server, select the type of algorithm, TKIP or AES, enter a password in the Pre-Shared key field of 8-64 characters, and enter a Group Key Renewal period time between 0 and 99,999 seconds, which instructs the Router or other device how often it should change the encryption keys.

WPA RADIUS. WPA used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router or other device.) First, select the type of WPA algorithm, **TKIP** or **AES**. Enter the RADIUS server's IP Address and port number, along with a key shared between the device and the server. Last, enter a Group Key Renewal period, which instructs the device how often it should change the encryption keys.

RADIUS. WEP used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router or other device.) First, enter the RADIUS server's IP Address and port number, along with a key shared between the device and the server. Then, select a WEP key and a level of WEP encryption, and either generate a WEP key through the Passphrase or enter the WEP key manually.

Implementing encryption may have a negative impact on your network's performance, but if you are transmitting sensitive data over your network, encryption should be used.

These security recommendations should help keep your mind at ease while you are enjoying the most flexible and convenient technology Linksys has to offer.

Appendix C: Windows Help

Almost all wireless products require Microsoft Windows. Windows is the most used operating system in the world and comes with many features that help make networking easier. These features can be accessed through Windows Help and are described in this appendix.

TCP/IP

Before a computer can communicate with an access point or wireless router, TCP/IP must be enabled. TCP/IP is a set of instructions, or protocol, all PCs follow to communicate over a network. This is true for wireless networks as well. Your PCs will not be able to utilize wireless networking without having TCP/IP enabled. Windows Help provides complete instructions on enabling TCP/IP.

Shared Resources

If you wish to share printers, folder, or files over your network, Windows Help provides complete instructions on utilizing shared resources.

Network Neighborhood/My Network Places

Other PCs on your network will appear under Network Neighborhood or My Network Places (depending upon the version of Windows you're running). Windows Help provides complete instructions on adding PCs to your network.

Appendix D: Glossary

802.11a - An IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps and an operating frequency of 5GHz.

802.11b - An IEEE wireless networking standard that specifies a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz.

802.11g - An IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps, an operating frequency of 2.4GHz, and backward compatibility with 802.11b devices.

Access Point - A device that allows wireless-equipped computers and other devices to communicate with a wired network. Also used to expand the range of a wireless network.

Adapter - A device that adds network functionality to your PC.

Ad-hoc - A group of wireless devices communicating directly with each other (peer-to-peer) without the use of an access point.

AES (**A**dvanced **E**ncryption **S**tandard) - A method that uses up to 256-bit key encryption to secure data.

Backbone - The part of a network that connects most of the systems and networks together, and handles the most data.

Bandwidth - The transmission capacity of a given device or network.

Beacon Interval - Data transmitted on your wireless network that keeps the network synchronized.

Bit - A binary digit.

Boot - To start a device and cause it to start executing instructions.

Bridge - A device that connects different networks.

Broadband - An always-on, fast Internet connection.

Browser - An application program that provides a way to look at and interact with all the information on the World Wide Web.

Buffer - A shared or assigned memory area that is used to support and coordinate different computing and networking activities so one isn't held up by the other.

Byte - A unit of data that is usually eight bits long

Cable Modem - A device that connects a computer to the cable television network, which in turn connects to the Internet.

CSMA/CA (**C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **A**voidance) - A method of data transfer that is used to prevent data collisions.

CTS (**C**lear **T**o **S**end) - A signal sent by a wireless device, signifying that it is ready to receive data.

Daisy Chain - A method used to connect devices in a series, one after the other.

Database - A collection of data that is organized so that its contents can easily be accessed, managed, and updated.

DDNS (**D**ynamic **D**omain **N**ame **S**ystem) - Allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (e.g., www.xyz.com) and a dynamic IP address.

Default Gateway - A device that forwards Internet traffic from your local area network.

DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) - A networking protocol that allows administrators to assign temporary IP addresses to network computers by “leasing” an IP address to a user for a limited amount of time, instead of assigning permanent IP addresses.

DMZ (**Dem**ilitarized **Z**one) - Removes the Router's firewall protection from one PC, allowing it to be “seen” from the Internet.

DNS (**D**omain **N**ame **S**erver) - The IP address of your ISP's server, which translates the names of websites into IP addresses.

Domain - A specific name for a network of computers.

Download - To receive a file transmitted over a network.

DSL (**D**igital **S**ubscriber **L**ine) - An always-on broadband connection over traditional phone lines.

DSSS (**D**irect-**S**equence **S**pread-**S**pectrum) - Frequency transmission with a redundant bit pattern resulting in a lower probability of information being lost in transit.

DTIM (**D**elivery **T**raffic **I**ndication **M**essage) - A message included in data packets that can increase wireless efficiency.

Dynamic IP Address - A temporary IP address assigned by a DHCP server.

EAP (**E**xtensible **A**uthentication **P**rotocol) - A general authentication protocol used to control network access. Many specific authentication methods work within this framework.

EAP-PEAP (**E**xtensible **A**uthentication **P**rotocol-**P**rotected **E**xtensible **A**uthentication **P**rotocol) - A mutual authentication method that uses a combination of digital certificates and another system, such as passwords.

EAP-TLS (**E**xtensible **A**uthentication **P**rotocol-**T**ransport **L**ayer **S**ecurity) - A mutual authentication method that uses digital certificates.

Encryption - Encoding data transmitted in a network.

Ethernet - IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium.

Finger - A program that tells you the name associated with an e-mail address.

Firewall - A set of related programs located at a network gateway server that protects the resources of a network from users from other networks.

Firmware - The programming code that runs a networking device.

Fragmentation -Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

FTP (**F**ile **T**ransfer **P**rotocol) - A protocol used to transfer files over a TCP/IP network.

Full Duplex - The ability of a networking device to receive and transmit data simultaneously.

Gateway - A device that interconnects networks with different, incompatible communications protocols.

Half Duplex - Data transmission that can occur in two directions over a single line, but only one direction at a time.

Hardware - The physical aspect of computers, telecommunications, and other information technology devices.

HTTP (**H**yper**T**ext **T**ransport **P**rotocol) - The communications protocol used to connect to servers on the World Wide Web.

IEEE (The **I**nstitute of **E**lectrical and **E**lectronics **E**ngineers) - An independent institute that develops networking standards.

Infrastructure - A wireless network that is bridged to a wired network via an access point.

IP (**I**nternet **P**rotocol) - A protocol used to send data over a network.

IP Address - The address used to identify a computer or device on a network.

IPCONFIG - A Windows 2000 and XP utility that displays the IP address for a particular networking device.

IPSec (**I**nternet **P**rotocol **Sec**urity) - A VPN protocol used to implement secure exchange of packets at the IP layer.

ISM band - Radio bandwidth utilized in wireless transmissions.

ISP (**I**nternet **S**ervice **P**rovider) - A company that provides access to the Internet.

LAN - The computers and networking products that make up your local network.

LEAP (**L**ightweight **E**xtensible **A**uthentication **P**rotocol) - A mutual authentication method that uses a username and password system.

MAC (**M**edia **A**ccess **C**ontrol) **Address** - The unique address that a manufacturer assigns to each networking device.

Mbps (**M**ega**B**its **P**er **S**econd) - One million bits per second; a unit of measurement for data transmission.

mIRC - An Internet Relay Chat program that runs under Windows.

Multicasting - Sending data to a group of destinations at once.

NAT (**N**etwork **A**ddress **T**ranslation) - NAT technology translates IP addresses of a local area network to a different IP address for the Internet.

Network - A series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users.

NNTP (**N**etwork **N**ews **T**ransfer **P**rotocol) - The protocol used to connect to Usenet groups on the Internet.

Node - A network junction or connection point, typically a computer or work station.

OFDM (**O**rthogonal **F**requency **D**ivision **M**ultiplexing) - Frequency transmission that separates the data stream into a number of lower-speed data streams, which are then transmitted in parallel to prevent information from being lost in transit.

Packet - A unit of data sent over a network.

Passphrase - Used much like a password, a passphrase simplifies the WEP encryption process by automatically generating the WEP encryption keys for Linksys products.

PEAP (**P**rotected **E**xtensible **A**uthentication **P**rotocol) - A mutual authentication method that uses a combination of digital certificates and another system, such as passwords.

Ping (**P**acket **IN**ternet **G**roper) - An Internet utility used to determine whether a particular IP address is online.

POP3 (**P**ost **O**ffice **P**rotocol **3**) - A standard mail server commonly used on the Internet.

Port - The connection point on a computer or networking device used for plugging in cables or adapters.

Power **o**ver **E**thernet (**PoE**) - A technology enabling an Ethernet network cable to deliver both data and power.

PPPoE (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet) - A type of broadband connection that provides authentication (username and password) in addition to data transport.

PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol) - A VPN protocol that allows the Point to Point Protocol (PPP) to be tunneled through an IP network. This protocol is also used as a type of broadband connection in Europe.

Preamble - Part of the wireless signal that synchronizes network traffic.

RADIUS (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice) - A protocol that uses an authentication server to control network access.

RJ-45 (**R**egistered **J**ack**-45**) - An Ethernet connector that holds up to eight wires.

Roaming - The ability to take a wireless device from one access point's range to another without losing the connection.

Router - A networking device that connects multiple networks together.

RTS (**R**equest **T**o **S**end) - A networking method of coordinating large packets through the RTS Threshold setting.

Server - Any computer whose function in a network is to provide user access to files, printing, communications, and other services.

SMTP (**S**imple **M**ail **T**ransfer **P**rotocol) - The standard e-mail protocol on the Internet.

SNMP (**S**imple **N**etwork **M**anagement **P**rotocol) - A widely used network monitoring and control protocol.

Software - Instructions for the computer. A series of instructions that performs a particular task is called a "program".

SOHO (**S**mall **O**ffice/**H**ome **O**ffice) - Market segment of professionals who work at home or in small offices.

SPI (**S**tateful **P**acket **I**nspection) **Firewall** - A technology that inspects every incoming packet of information before allowing it to enter the network.

Spread Spectrum - Wideband radio frequency technique used for more reliable and secure data transmission.

SSID (**S**ervice **S**et **ID**entifier) - Your wireless network's name.

Static IP Address - A fixed address assigned to a computer or device that is connected to a network.

Static Routing - Forwarding data in a network via a fixed path.

Subnet Mask - An address code that determines the size of the network.

Switch - 1. A data switch that connects computing devices to host computers, allowing a large number of devices to share a limited number of ports. 2. A device for making, breaking, or changing the connections in an electrical circuit.

TCP (**T**ransmission **C**ontrol **P**rotocol) - A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol) - A set of instructions PCs use to communicate over a network.

Telnet - A user command and TCP/IP protocol used for accessing remote PCs.

TFTP (**T**rivial **F**ile **T**ransfer **P**rotocol) - A version of the TCP/IP FTP protocol that has no directory or password capability.

Throughput - The amount of data moved successfully from one node to another in a given time period.

TKIP (**T**emporal **K**ey **I**ntegrity **P**rotocol) - a wireless encryption protocol that provides dynamic encryption keys for each packet transmitted.

Topology - The physical layout of a network.

TX Rate - Transmission Rate.

UDP (**U**ser **D**atagram **P**rotocol) - A network protocol for transmitting data that does not require acknowledgement from the recipient of the data that is sent.

Upgrade - To replace existing software or firmware with a newer version.

Upload - To transmit a file over a network.

URL (**U**niform **R**esource **L**ocator) - The address of a file located on the Internet.

VPN (**V**irtual **P**rivate **N**etwork) - A security measure to protect data as it leaves one network and goes to another over the Internet.

WAN (**W**ide **A**rea **N**etwork)- The Internet.

WEP (**W**ired **E**quivalent **P**rivacy) - A method of encrypting network data transmitted on a wireless network for greater security.

WINIPCFG - A Windows 98 and Me utility that displays the IP address for a particular networking device.

WLAN (**W**ireless **L**ocal **A**rea **N**etwork) - A group of computers and associated devices that communicate with each other wirelessly.

WPA (**W**i-Fi **P**rotected **A**ccess) - a wireless security protocol using TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.

Appendix E: Specifications

Model	WUSB54GP
Standards	IEEE 802.11b, IEEE 802.11g, USB 1.1, USB 2.0
Cabling Type	USB extension base with integrated USB Cable
LEDs	Link (Blue- Blinking when 802.11g RF signal is active)
Frequency Band	2.400~2.4835GHz (Subject to local regulation)
Peak Gain of Antenna	2.4 GHz => 2dBi
Transmit Power	15 dBm (Typical)@11Mbps DSSS 14 dBm (Typical)@54Mbps OFDM
Receive Sensitivity	802.11g: 11Mbps @ -83dBm, 54Mbps @-67dBm
Data Rate	11,5.5,2, 1Mbs auto-selection on 802.11b 54,48,36,24,18,12,9,6 Mbps auto-selection on 802.11g
Channels	802.11b / 802.11g 11 Channels (US, Canada) 13 Channels (Europe) 14 Channels (Japan)
OS Support	Windows 98SE, Me, 2000 or XP with Service Pack 1 (or later)
Security Features	WEP (64 and 128-bit), WPA, AES, TKIP, 802.1x
Dimensions	1.25" x 4.5" x 0.38" (31.75 mm x 114.3 mm x 9.525 mm)
Unit Weight	4.50 oz. (0.128 kg)

Certifications	FCC
Operating Temp.	32ºF to 104ºF (0ºC to 40ºC)
Storage Temp.	-40ºF to 158ºF (-40ºC to 70ºC)
Operating Humidity	10% to 85%, Non-Condensing
Storage Humidity	5% to 90%, Non-Condensing

Appendix F: Warranty Information

LIMITED WARRANTY

Linksys warrants to You that, for a period of three years (the “Warranty Period”), your Linksys Product will be substantially free of defects in materials and workmanship under normal use. Your exclusive remedy and Linksys' entire liability under this warranty will be for Linksys at its option to repair or replace the Product or refund Your purchase price less any rebates. This limited warranty extends only to the original purchaser.

If the Product proves defective during the Warranty Period call Linksys Technical Support in order to obtain a Return Authorization Number, if applicable. BE SURE TO HAVE YOUR PROOF OF PURCHASE ON HAND WHEN CALLING. If You are requested to return the Product, mark the Return Authorization Number clearly on the outside of the package and include a copy of your original proof of purchase. RETURN REQUESTS CANNOT BE PROCESSED WITHOUT PROOF OF PURCHASE. You are responsible for shipping defective Products to Linksys. Linksys pays for UPS Ground shipping from Linksys back to You only. Customers located outside of the United States of America and Canada are responsible for all shipping and handling charges.

ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE ARE LIMITED TO THE DURATION OF THE WARRANTY PERIOD. ALL OTHER EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF NON-INFRINGEMENT, ARE DISCLAIMED. Some jurisdictions do not allow limitations on how long an implied warranty lasts, so the above limitation may not apply to You. This warranty gives You specific legal rights, and You may also have other rights which vary by jurisdiction.

This warranty does not apply if the Product (a) has been altered, except by Linksys, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Linksys, or (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Linksys does not warrant that the Product will be free of vulnerability to intrusion or attack.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL LINKSYS BE LIABLE FOR ANY LOST DATA, REVENUE OR PROFIT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, REGARDLESS OF THE THEORY OF LIABILITY (INCLUDING NEGLIGENCE), ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE THE PRODUCT (INCLUDING ANY SOFTWARE), EVEN IF LINKSYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL LINKSYS’ LIABILITY EXCEED THE AMOUNT PAID BY YOU FOR THE PRODUCT. The foregoing limitations will apply even if any warranty or remedy provided under this Agreement fails of its essential purpose. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to You.

Please direct all inquiries to: Linksys, P.O. Box 18558, Irvine, CA 92623.

Appendix G: Regulatory Information

FCC STATEMENT

This product has been tested and complies with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which is found by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

Reorient or relocate the receiving antenna

Increase the separation between the equipment or devices

Connect the equipment to an outlet other than the receiver's

Consult a dealer or an experienced radio/TV technician for assistance

FCC Radiation Exposure Statement
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.

INDUSTRY CANADA (CANADA)

This Class B digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.
The use of this device in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations.

EC DECLARATION OF CONFORMITY (EUROPE)

Linksys declares that this product conforms to the specifications listed below, following the provisions of the European R&TTE directive 1999/5/EC:

EN 301 489-1, 301 489-17 General EMC requirements for Radio equipment.

EN 609 50 Safety

EN 300-328-1, EN 300-328-2 Technical requirements for Radio equipment.

Caution: This equipment is intended to be used in all EU and EFTA countries. Outdoor use may be restricted to certain frequencies and/or may require a license for operation. Contact local Authority for procedure to follow.

Note: Combinations of power levels and antennas resulting in a radiated power level of above 100 mW equivalent isotropic radiated power (EIRP) are considered as not compliant with the above mentioned directive and are not allowed for use within the European community and countries that have adopted the European R&TTE directive 1999/5/EC.

For more details on legal combinations of power levels and antennas, contact Linksys Corporate Compliance.

Linksys vakuuttaa täten että dieses produkt tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien näiden direktiivien muiden ehtojen mukainen.

Linksys déclare que le produit est conforme aux conditions essentielles et aux dispositions relatives à la directive 1999/5/EC.

Belgique:

Dans le cas d'une utilisation privée, à l'extérieur d'un bâtiment, au-dessus d'un espace public, aucun enregistrement n'est nécessaire pour une distance de moins de 300m. Pour une distance supérieure à 300m un enregistrement auprès de l'IBPT est requise. Pour une utilisation publique à l'extérieur de bâtiments, une licence de l'IBPT est requise. Pour les enregistrements et licences, veuillez contacter l'IBPT.

France:

2.4 GHz Bande : les canaux 10, 11, 12, 13 (2457, 2462, 2467, et 2472 MHz respectivement) sont complétement libres d'utilisation en France (en utilisation intérieur). Pour ce qui est des autres canaux, ils peuvent être soumis à autorisation selon le département. L'utilisation en extérieur est soumis à autorisation préalable et très restreint.

Vous pouvez contacter l'Autorité de Régulation des Télécommunications (http://www.art-telecom.fr) pour de plus amples renseignements.

Appendix H: Contact Information

Need to contact Linksys? Visit us online for information on the latest products and updates to your existing products at:	http://www.linksys.com or ftp.linksys.com
Can't find information about a product you want to buy on the web? Do you want to know more about networking with Linksys products? Give our advice line a call at:	800-546-5797 (LINKSYS)
Or fax your request in to:	949-823-3002
If you experience problems with any Linksys product, you can call us at:	800-326-7114
Don't wish to call? You can e-mail us at:	support@linksys.com
If any Linksys product proves defective during its warranty period, you can call the Linksys Return Merchandise Authorization department for obtaining a Return Authorization Number at: (Details on Warranty and RMA issues can be found in the Warranty Information section in this Guide.)	949-823-3000